100 XP

# Introduction

1 minute

**When it comes to security, your organization can no longer rely on its network boundary. To allow employees, partners, and customers to collaborate securely, organizations need to shift to an approach whereby identity becomes the new security perimeter. Using an identity provider helps organizations manage that shift and all the aspects of identity security.**

**In this module, you'll learn about Microsoft Entra ID, Microsoft's cloud-based identity and access management service. You'll also learn about the identity types supported and how you can use Microsoft Entra ID to support external users.**

**After completing this module, you'll be able to:**

- **Describe the core functionality of Microsoft Entra ID.**
- **Describe the types of identities supported by Microsoft Entra ID**
- **Describe the concept of hybrid identity as supported by Microsoft Entra ID.**

## Next unit: Describe Microsoft Entra ID

Continue

**How are we doing?** ☆ ☆ ☆ ☆ ☆

100 XP

# Describe Microsoft Entra ID

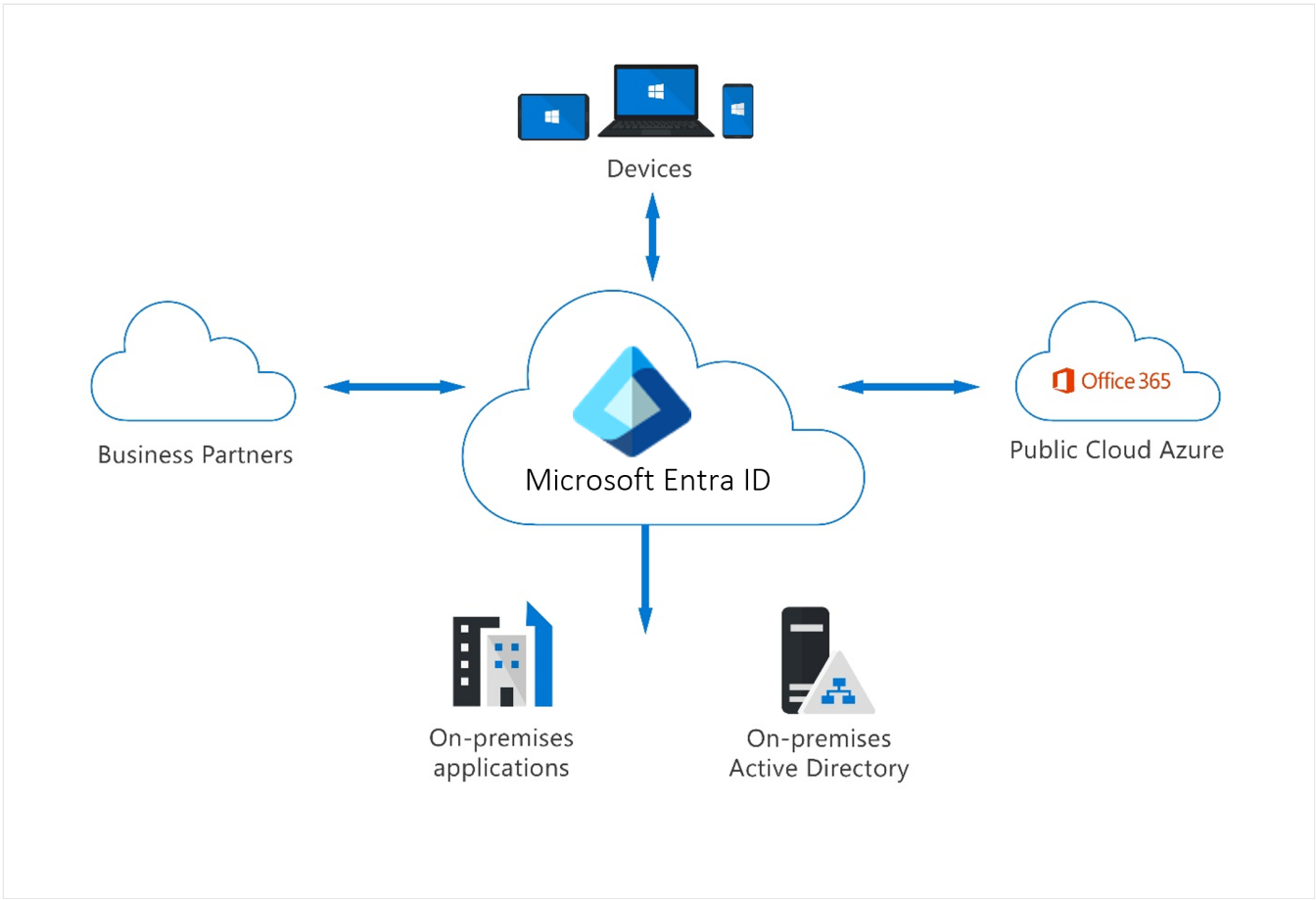
2 minutes

**Microsoft Entra ID, formerly Azure Active Directory, is Microsoft's cloud-based identity and access management service. Organizations use Microsoft Entra ID to enable their employees, guests, and others to sign in and access the resources they need, including:**

- **Internal resources, such as apps on your corporate network and intranet, and cloud apps developed by your own organization.**
- **External services, such as Microsoft Office 365, the Azure portal, and any SaaS applications used by your organization.**

**Microsoft Entra ID simplifies the way organizations manage authorization and access by providing a single identity system for their cloud and on-premises applications. Microsoft Entra ID can be synchronized with your existing on-premises Active Directory, synchronized with other directory services, or used as a standalone service.**

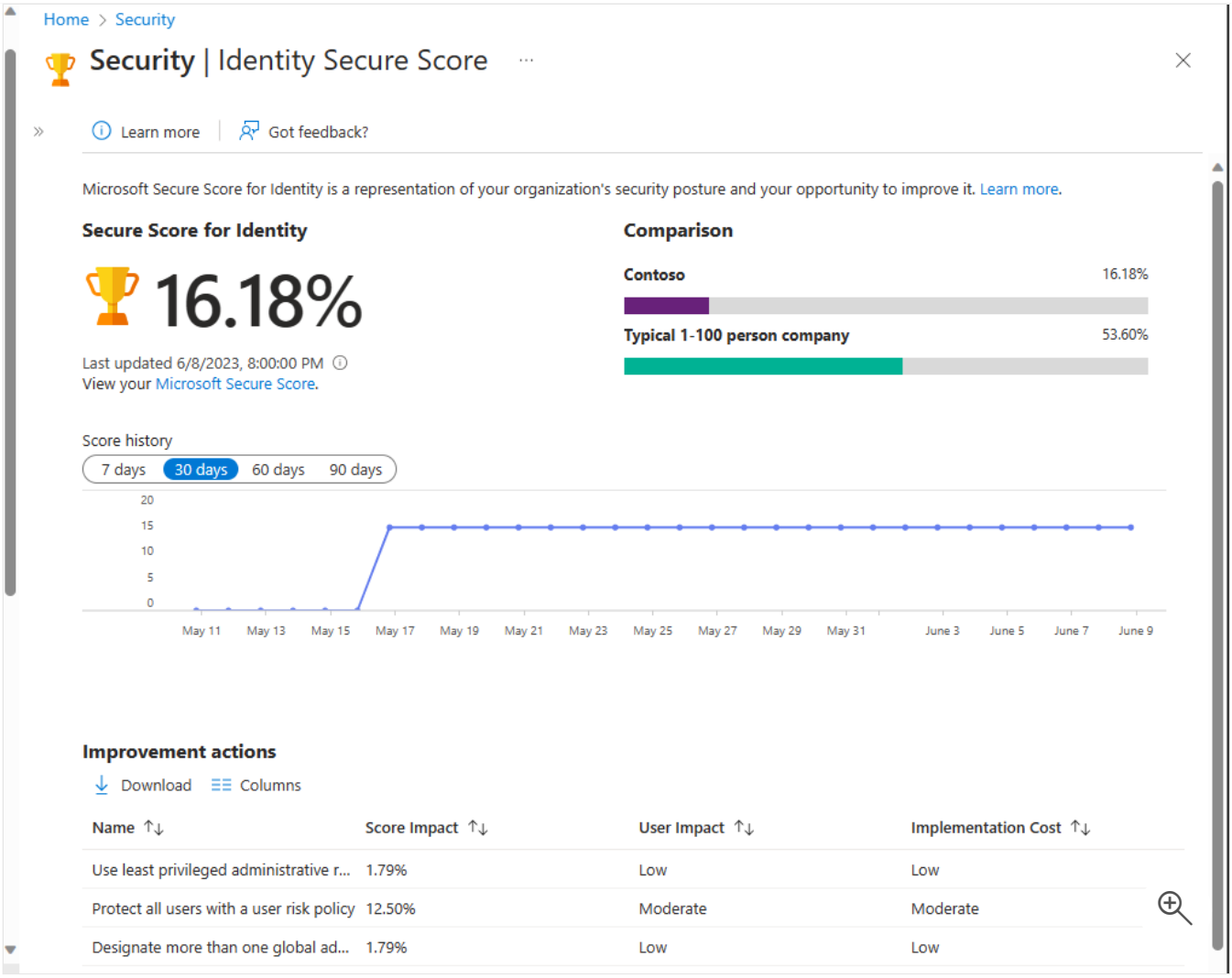
**Microsoft Entra ID also allows organizations to securely enable the use of personal devices, such as mobiles and tablets, and enable collaboration with business partners and customers.**




## Identity Secure Score

**Microsoft Entra ID includes an identity secure score, which is a percentage that functions as an indicator for how aligned you are with Microsoft's best practice recommendations for security. Each improvement action in identity secure score is tailored to your specific configuration.**

**Identity secure score, which is available in all editions of Microsoft Entra ID, helps you to objectively measure your identity security posture, plan identity security improvements, and review the success of your improvements.**




# Basic terminology

**When talking about Microsoft Entra ID, there's some basic terminology that is important to understand.**

- ***Tenant*** **- A Microsoft Entra ID tenant is an instance of Microsoft Entra in which information about a single organization resides including organizational objects such as users, groups, devices, and application registrations. A tenant also contains access and compliance policies for resources, such as applications registered in the directory. Each Microsoft Entra ID tenant has a unique ID (tenant ID) and a domain name (for example, contoso.onmicrosoft.com) and serves as a security and administrative boundary, allowing the organization to manage and control access to resources, applications, devices, and services.**

- ***Directory*** **- The terms Microsoft Entra ID directory and Microsoft Entra ID tenant are often used interchangeably. The directory is a logical container within a Microsoft Entra ID tenant that holds and organizes the various resources and objects related to identity and access management including users, groups, applications, devices, and other directory objects. Basically, the directory is like a**

**database or catalog of identities and resources associated with an organization's tenant. A Microsoft Entra ID tenant consists of only one directory.**

- ***Multi-tenant*** **- A multi-tenant organization is an organization that has more than one instance of Microsoft Entra ID. Reasons why an organization might have multiple tenants include organizations with multiple subsidiaries or business units that operate independently, organizations that merge or acquire companies, multiple geographical boundaries with various residency regulations, and more.**

## Who uses Microsoft Entra ID?

**Microsoft Entra ID is used by IT admins to control access to corporate apps and resources, based on business requirements. For example, Microsoft Entra ID can also be set up to require multi-factor authentication when accessing important organizational resources. It provides powerful tools to automatically help protect user identities and credentials and to meet an organization's access governance requirements.**

**Developers use Microsoft Entra ID as a standards-based approach for adding single sign-on (SSO) to their apps, so that users can sign in with their pre-existing credentials. Microsoft Entra ID also provides application programming interfaces (APIs) that allow developers to build personalized app experiences using existing organizational data.**

**Subscribers to Azure services, Microsoft 365, or Dynamics 365 automatically have access to Microsoft Entra ID. Users of these services can take advantage of included services and can also enhance their Microsoft Entra ID implementation by upgrading to premium licenses.**

---

## Next unit: Describe types of identities

Continue >

---

**How are we doing?** ☆ ☆ ☆ ☆ ☆

100 XP

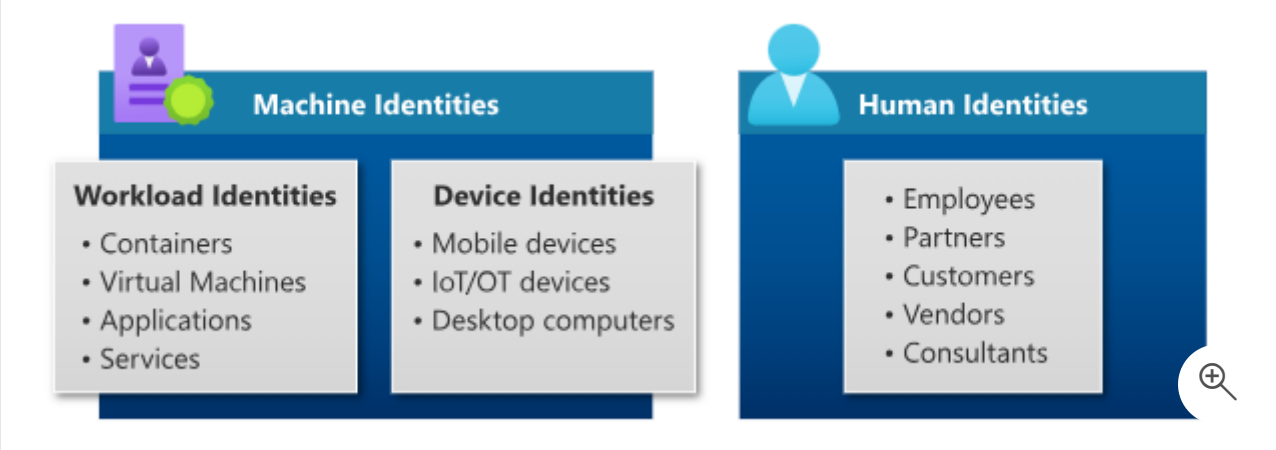
# Describe types of identities

8 minutes

**In Microsoft Entra ID, there are different types of identities that are supported. The terms you'll hear and are introduced in this unit are user identities, workload identities, device identities, external identities, and hybrid identities. Each of these terms is described in more detail in the sections that follow.**

**When you ask the question, to what can I assign an identity in Microsoft Entra ID, there are three categories.**

- **You can assign identities to people (humans). Examples of identities assigned to people are employees of an organization that are typically configured as internal users, and external users that include customers, consultants, vendors, and partners. For our purposes, we'll refer to these as user identities.**
- **You can assign identities to physical devices, such as mobile phones, desktop computers, and IoT devices.**
- **Lastly, you can assign identities to software-based objects, such as applications, virtual machines, services, and containers. These identities are referred to as workload identities.**




**In this unit, we consider each type of Microsoft Entra ID identity.**

## User

**User identities represent people such as employees and external users (customers, consultants, vendors, and partners). In Microsoft Entra ID, user identities are characterized by how they authenticate and the user type property.**

**How the user authenticates is asked relative to the host organization's Microsoft Entra ID tenant and can be internal or external. Internal authentication means the user has an account on the host organization's Microsoft Entra ID and uses that account to authenticate to Microsoft Entra ID. External authentication means the user authenticates using an external Microsoft Entra ID account that belongs to another organization, a social network identity, or other external identity provider.**

**The user type property describes the user's relationship to the organization or more specifically, the host organization's tenancy. The user can be a guest or a member of the organization's Microsoft Entra ID tenant. By default, guests of the organization have limited privileges in the organization's directory, relative to members of the organization.**

| | | UserType property | |
|---|---|---|---|
| | | Guest | Member |
| How the user authenticates | External  | External guest<br><br>Uses an external Microsoft Entra ID account, social identity, or other external identity provider to sign in.<br><br>Most external users fall into this category. | External member<br><br>Uses an external account to authenticate but has member-level access in your organization.<br><br>Common scenario in multi-tenant organizations. |
| | Internal  | Internal guest<br><br>Has an account in your Microsoft Entra ID directory but only guest-level access in your organization.<br><br>This is often a legacy user created before the availability of Microsoft Entra B2B. | Internal member<br><br>Has an account in your Microsoft Entra ID directory and member-level access in your organization.<br><br>Generally considered employees of your organization. |

- **Internal member: These users are typically considered employees of your organization. The user authenticates internally via their organization's Microsoft Entra ID, and the user object created in the resource Microsoft Entra ID directory has a UserType of Member.**
- **External guest: External users or guests, including consultants, vendors, and partners, typically fall into this category. The user authenticates using an external Microsoft Entra ID account or an external identity provider (such as a social identity). The user object created in the resource Microsoft Entra ID directory has a UserType of Guest, giving them limited, guest-level permissions.**

- **External member: This scenario is common in organizations consisting of multiple tenants. Consider the scenario where the Contoso Microsoft Entra ID tenant and the Fabrikam Microsoft Entra ID tenant are tenants within one large organization. Users from the Contoso tenant need member level access to resources in Fabrikam. In this scenario, Contoso users are configured in the Fabrikam Microsoft Entra ID directory such that they authenticate with their Contoso account, which is external to Fabrikam, but have a UserType of Member to enable member-level access to Fabrikam's organizational resources.**
- **Internal guest: This scenario exists when organizations who collaborate with distributors, suppliers, and vendors set up internal Microsoft Entra ID accounts for these users but designate them as guests by setting the user object UserType to Guest. As a guest, they have reduced permissions in the directory. This is considered a legacy scenario as it is now more common to use B2B collaboration. With B2B collaboration users can use their own credentials, allowing their external identity provider to manage authentication and their account lifecycle.**

**External guests and external members are business-to-business (B2B) collaboration users that fall under the category of external identities in Microsoft Entra ID and is described in more detail in the subsequent unit.**

**In the following interactive guide, you'll add a new user to Microsoft Entra ID. Select the image that follows to get started and follow the prompts on the screen.**


## Workload identities

**A workload identity is an identity you assign to a software workload. This enables the software workload to authenticate to and access other services and resources. This helps secure your workload. In Microsoft Entra, workload identities are applications, service principals, and managed identities.**

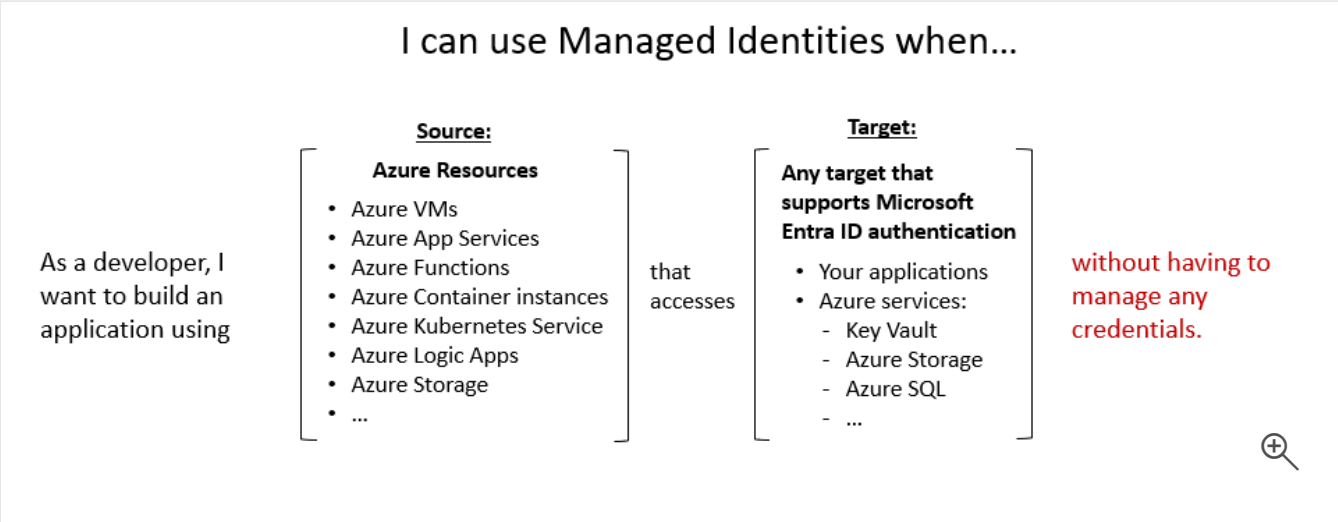
## Applications and service principals

**A service principal is essentially, an identity for an application. For an application to delegate its identity and access functions to Microsoft Entra ID, the application must first be registered with Microsoft Entra ID to enable its integration. Once an application is registered, a service principal is created in each Microsoft Entra ID tenant where the application is used. The service principal enables core features such as authentication and authorization of the application to resources that are secured by the Microsoft Entra ID tenant.**

**For the service principals to be able to access resources secured by the Microsoft Entra ID tenant, application developers must manage and protect the credentials. If not done correctly, this can introduce security vulnerabilities. Managed identities help offload that responsibility from the developer.**

## Managed identities

**Managed identities are a type of service principal that are automatically managed in Microsoft Entra ID and eliminate the need for developers to manage credentials. Managed identities provide an identity for applications to use when connecting to Azure resources that support Microsoft Entra ID authentication and can be used without any extra cost.**




**For a list of Azure Services that support managed identities, refer to the Learn more section of the Summary and resources unit.**

**There are two types of managed identities: system-assigned and user-assigned.**

- **System-assigned. Some Azure resources, such as virtual machines, allow you to enable a managed identity directly on the resource. When you enable a system-assigned managed identity an identity is created in Microsoft Entra ID that's tied to the lifecycle of that Azure resource. Because the identity is tied to the lifecycle of that Azure resource when the resource is deleted, Azure automatically deletes the identity for you. An example where you may find a system-assigned identity is when a workload is contained within a single Azure resource, such as an application that runs on a single virtual machine.**
- **User-assigned. You may also create a managed identity as a standalone Azure resource. Once you create a user-assigned managed identity, you can assign it to one or more instances of an Azure service. For example, a user-assigned managed identity can be assigned to multiple VMs. With user-assigned managed identities, the identity is managed separately from the resources that use it. Deleting the resources that use the user-assigned managed identity doesn't delete the identity. The user-assigned managed identity must be explicitly deleted. This is useful in a scenario where you may have multiple VMs that all have the same set of permissions but may get recycled frequently. Deleting any of the VMs doesn't impact the user-assigned managed identity. Similarly, you can create a new VM and assign it the existing user-assigned managed identity.**

## Device

**A device is a piece of hardware, such as mobile devices, laptops, servers, or printers. A device identity gives administrators information they can use when making access or configuration decisions. Device identities can be set up in different ways in Microsoft Entra ID.**

- **Microsoft Entra ID registered devices. The goal of Microsoft Entra ID registered devices is to provide users with support for bring your own device (BYOD) or mobile device scenarios. In these scenarios, a user can access your organization's resources using a personal device. Microsoft Entra ID registered devices register to Microsoft Entra ID without requiring an organizational account to sign in to the device.**
- **Microsoft Entra ID joined. A Microsoft Entra ID joined device is a device joined to Microsoft Entra ID through an organizational account, which is then used to sign in to the device. Microsoft Entra ID joined devices are generally owned by the organization.**
- **Hybrid Microsoft Entra ID joined devices. Organizations with existing on-premises Active Directory implementations can benefit from the functionality provided by**

**Microsoft Entra ID by implementing hybrid Microsoft Entra ID joined devices. These devices are joined to your on-premises Active Directory and Microsoft Entra ID requiring organizational account to sign in to the device.**

**Registering and joining devices to Microsoft Entra ID gives users Single Sign-on (SSO) to cloud-based resources. Additionally, devices that are Microsoft Entra ID joined benefit from the SSO experience to resources and applications that rely on on-premises Active Directory.**

**IT admins can use tools like Microsoft Intune, a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM), to control how an organization's devices are used. For more information, see Microsoft Intune.**

## Groups

**In Microsoft Entra ID, if you have several identities with the same access needs, you can create a group. You use groups to give access permissions to all members of the group, instead of having to assign access rights individually. Limiting access to Microsoft Entra ID resources to only those identities who need access is one of the core security principles of Zero Trust.**

**There are two group types:**

- **Security: A security group is the most common type of group and it's used to manage user and device access to shared resources. For example, you may create a security group for a specific security policy such as Self-service password reset or for use with a conditional access policy to require MFA. Members of a security group can include users (including external users), devices, other groups, and service principals. Creating security groups requires a Microsoft Entra ID administrator role.**
- **Microsoft 365: A Microsoft 365 group, which is also often referred to as a distribution group, is used for grouping users according to collaboration needs. For example, you can give members of the group access to a shared mailbox, calendar, files SharePoint sites, and more. Members of a Microsoft 365 group can only include users, including users outside of your organization. Because Microsoft 365 groups are intended for collaboration, the default is to allow users to create Microsoft 365 groups, so you don't need an administrator role.**

**Groups can be configured to allow members to be assigned, that is manually selected, or they can be configured for dynamic membership. Dynamic membership uses rules to automatically add and remove identities.**

## Next unit: Describe hybrid identity

Continue >

**How are we doing?** ☆ ☆ ☆ ☆ ☆

100 XP

# Describe hybrid identity

6 minutes

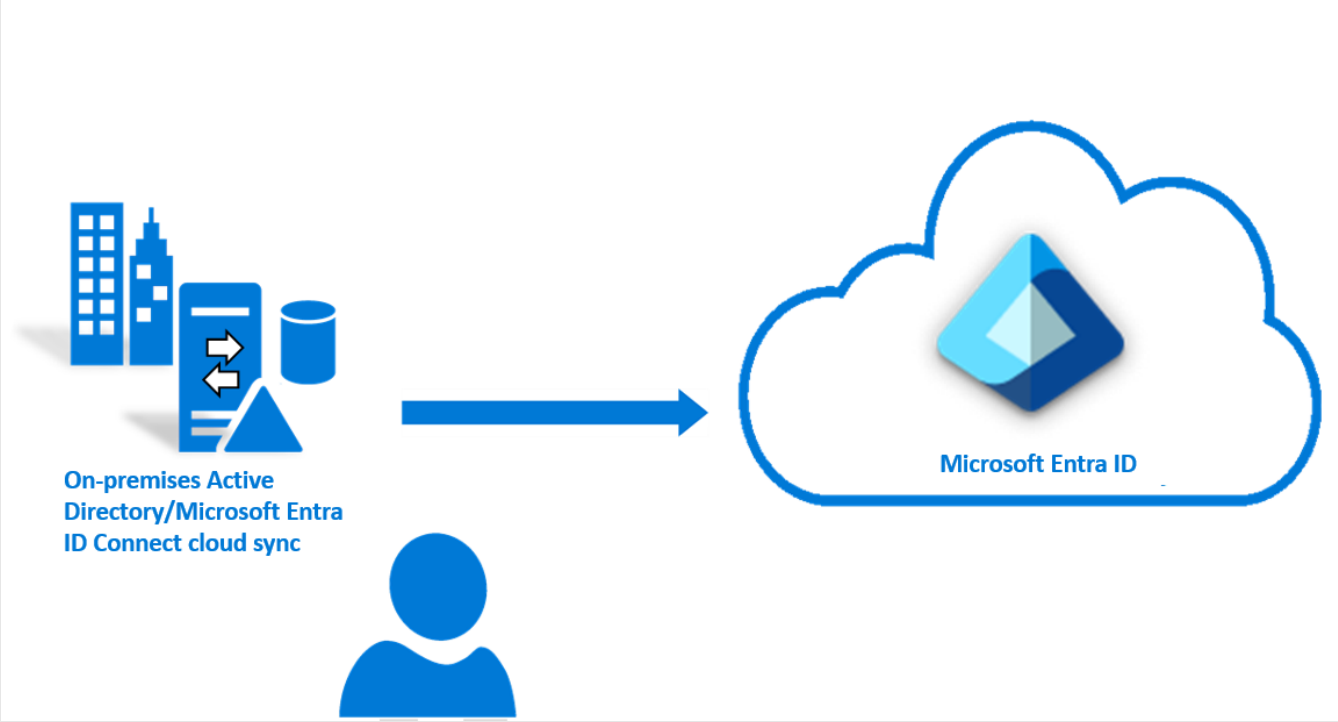
**While there's no denying the rapid pace at which organizations are moving their workloads to the cloud, many businesses, and corporations are still a mixture of on-premises and cloud applications. Regardless of where an application is hosted, users expect and require easy access. As such, there's need to have a single identity across these various applications.**

**Microsoft's identity solutions span on-premises and cloud-based capabilities. These solutions create a common identity for authentication and authorization to all resources, regardless of location. We call this hybrid identity.**

**Hybrid identity is accomplished through provisioning and synchronization.**

- **Inter-directory provisioning is provisioning an identity between two different directory services systems. For a hybrid environment, the most common scenario for inter-directory provisioning is when a user already in Active Directory is provisioned into Microsoft Entra ID.**
- **Synchronization is responsible for making sure identity information for your on-premises users and groups is matching the cloud.**

**One of the available methods for accomplishing inter-directory provisioning and synchronization is through Microsoft Entra ID Connect cloud sync. Microsoft Entra ID Connect cloud sync is designed to meet and accomplish your hybrid identity goals for the provisioning and synchronization of users, groups, and contacts to Microsoft Entra ID. It accomplishes this by using the Microsoft Entra ID cloud provisioning agent. The agent provides a lightweight inter-directory provisioning experience that acts as a bridge between Microsoft Entra ID and Active Directory. An organization only needs to deploy the agent in their on-premises or IaaS-hosted environment. The provisioning configuration is stored in Microsoft Entra ID and managed as part of the service.**




**The Microsoft Entra ID Connect cloud sync provisioning agent uses the System for Cross-domain Identity Management (SCIM) specification with Microsoft Entra ID to provision and deprovision users and groups. The SCIM specification is a standard that is used to automate the exchanging of user or group identity information between identity domains such as Microsoft Entra ID and is becoming the de facto standard for provisioning.**

## Next unit: Describe external identities

Continue >

**How are we doing?** ☆ ☆ ☆ ☆ ☆

100 XP

# Describe external identities

3 minutes

**Today's world is about collaboration, working with people both inside and outside of your organization. That means you'll sometimes need to provide access to your organization's applications or data to external users.**

**Microsoft Entra ID External Identities refers to all the ways you can securely interact with users outside of your organization.**

**The following capabilities make up External Identities:**

- **B2B collaboration**
- **B2B direct connect**
- **Microsoft Entra External ID for customers (preview)**
- **Microsoft Entra ID multi-tenant organization**

## B2B collaboration

**B2B collaboration enables employees of an organization to collaborate with external users by letting them use their preferred identity to sign in to your Microsoft applications or other enterprise applications. B2B collaboration users are represented in your directory, typically as guest users.**

**There are no credentials associated with B2B collaboration users. Instead, they authenticate with their home organization or identity provider, and then your organization checks the guest user's eligibility for B2B collaboration.**

**There are various ways to add external users to your organization for B2B collaboration:**

- **Invite users to B2B collaboration using their Microsoft Entra ID accounts, Microsoft accounts, or social identities that you enable. The user signs into the shared resources using a simple redemption process with their work, school, or other email account.**
- **Use self-service sign-up user flows to let external users sign up for applications themselves. The experience can be customized to allow sign-up with a work, school, or social identity. You can also collect information about the user during the sign-up process.**

- **Use Microsoft Entra ID entitlement management, an identity governance feature that lets you manage identity and access for external users at scale by automating access request workflows, access assignments, reviews, and expiration.**

**A user object is created for the B2B collaboration user in the same directory as your employees. This user object can be managed like other user objects in your directory, added to groups, and so on. You can assign permissions to the user object (for authorization) while letting them use their existing credentials (for authentication).**

**You can manage B2B collaboration with other Microsoft Entra ID organizations and across Microsoft Azure clouds by using cross-tenant access settings that give you granular control over how external Microsoft Entra ID organizations collaborate with you (inbound access) and how your users collaborate with external Microsoft Entra ID organizations (outbound access). You can also use external collaboration settings to manage B2B collaboration with non-Microsoft Entra ID external users and organizations.**

## B2B direct connect

**B2B direct connect is a new way to collaborate with other Microsoft Entra ID organizations using Microsoft Teams shared channels. With B2B direct connect, you create two-way trust relationships with other Microsoft Entra ID organizations to allow users to seamlessly sign in to your shared resources and vice versa. B2B direct connect users aren't represented in your Microsoft Entra ID directory (they aren't added as guests), but they're visible from within the Teams shared channel and can be monitored in Teams admin center reports. When two organizations mutually enable B2B direct connect, users authenticate in their home organization and receive a token from the resource organization for access.**

**B2B direct connect enables the Teams Connect shared channels feature, which lets your users collaborate with external users from multiple organizations with a Teams shared channel for chat, calls, file-sharing, and app-sharing. Once you've set up B2B direct connect with an external organization, the following Teams shared channels capabilities become available:**

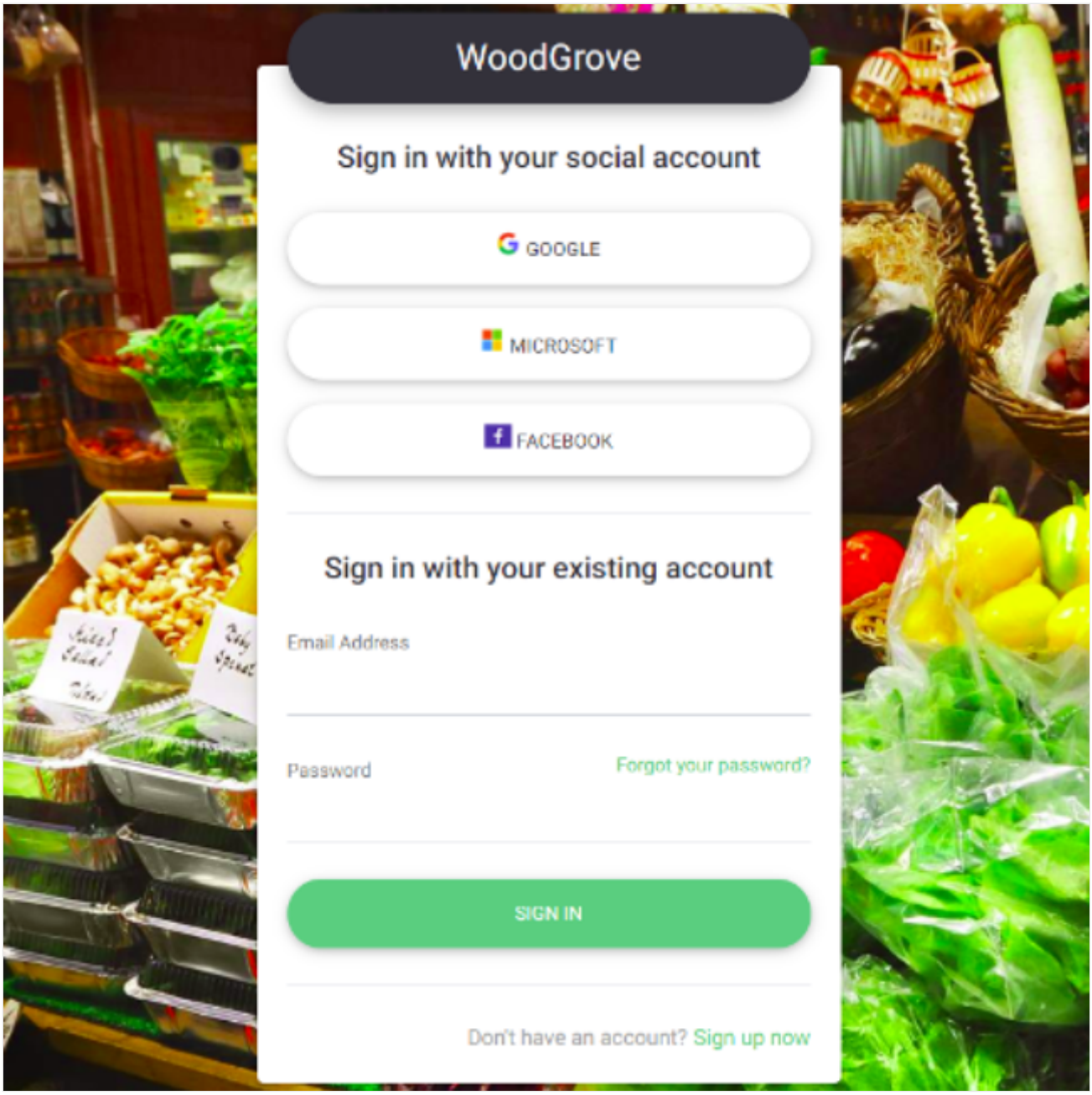
- **Within Teams, a shared channel owner can search for allowed users from the external organization and add them to the shared channel.**
- **External users can access the Teams shared channel without having to switch organizations or sign in with a different account. From within Teams, the external user can access files and apps through the Files tab. The user's access is determined by the shared channel's policies. You use cross-tenant access settings to manage trust relationships with other Microsoft Entra ID organizations and define inbound and outbound policies for B2B direct connect.**

# Microsoft Entra External ID for customers (Preview)

**Microsoft Entra External ID for customers is Microsoft's new customer identity and access management (CIAM) solution. This solution is intended for businesses that want to make applications available to their customers using the Microsoft Entra platform for identity and access.**

**With Microsoft Entra External ID for customers, you create a distinct tenant that follows the standard Microsoft Entra ID tenant model but is configured for customer scenarios. Capabilities include:**

- **Single sign-on (SSO) with social and enterprise identities. Customers can choose a social, enterprise, or managed identity to sign in with a username and password, email, or one-time passcode.**
- **Sign-up and sign-in pages to your apps. Quickly add intuitive, user-friendly sign-up and sign-in experiences for your customer apps.**
- **Add your company branding to the sign-up page. Customize the look and feel of your sign-up and sign-in experiences. With a single identity, a customer can securely access all the applications you want them to use.**
- **Provide self-service account management. Customers can register for your online services by themselves, manage their profile, delete their account, enroll in a multifactor authentication (MFA) method, or reset their password with no admin or help desk assistance.**




## Multi-tenant organizations

**A multi-tenant organization is an organization that has more than one instance of Microsoft Entra ID. There are various reasons for multi-tenancy, like using multiple clouds or having multiple geographical boundaries. Multi-tenant organizations use a one-way synchronization service in Microsoft Entra ID, called cross-tenant synchronization. Cross-tenant synchronization enables seamless collaboration for a multi-tenant organization. It improves user experience and ensures that users can access resources, without receiving an invitation email and having to accept a consent prompt in each tenant.**

## Next unit: Knowledge check

Continue >

**How are we doing?** ☆ ☆ ☆ ☆ ☆

100 XP

# Summary & resources

1 minute

**In this module, you've gained an insight into the core functionality of Microsoft Entra ID and the identity types supported. You also learned about the concept of a hybrid identity model, where all user identities are managed in your on-premises Active Directory Domain Services (AD DS) directory, and changes are synchronized to your Azure AD.**

**Now that you've completed this module, you'll be able to:**

- **Describe the core functionality of Microsoft Entra ID.**
- **Describe the types of identities supported by Microsoft Entra ID**
- **Describe the concept of hybrid identity as supported by Microsoft Entra ID.**

## Learn more

**For more information on the topics covered in this module, see:**

- What is Microsoft Entra ID?
- What is a multi-tenant organization in Microsoft Entra ID?
- What is identity secure score?
- What are workload identities?
- Application and service principal objects in Microsoft Entra ID
- What are managed identities for Azure resources?
- Services that support managed identities for Azure resources
- External Identities in Microsoft Entra ID
- B2B collaboration overview
- Properties of a B2B collaboration user
- What is Microsoft Entra External ID for customers?
- Microsoft Entra ID registered devices
- Microsoft Entra ID joined devices
- Hybrid Microsoft Entra ID joined devices

## Explore other modules

Microsoft Security, Compliance, and Identity Fundamentals: Describe the capabilities of Microsoft Entra

# MS-900 Microsoft 365 Fundamentals: Describe Microsoft 365 security and compliance capabilities

**How are we doing?** ☆ ☆ ☆ ☆ ☆

100 XP

# Introduction

1 minute

**Authentication is the process of verifying an identity to be legitimate. Passwords are commonly used to authenticate users, but there are better and more secure ways to authenticate.**

**In this module, you'll learn about the authentication capabilities of Microsoft Entra ID, multifactor authentication, and how it improves security. You'll also find out about the password protection and management capabilities of Microsoft Entra ID.**

**After completing this module, you'll be able to:**

- **Describe the authentication methods of Microsoft Entra ID.**
- **Describe multifactor authentication in Microsoft Entra ID**
- **Describe the password protection and management capabilities of Microsoft Entra ID.**

## Next unit: Describe authentication methods

Continue

**How are we doing?** ☆ ☆ ☆ ☆ ☆

100 XP

# Describe authentication methods

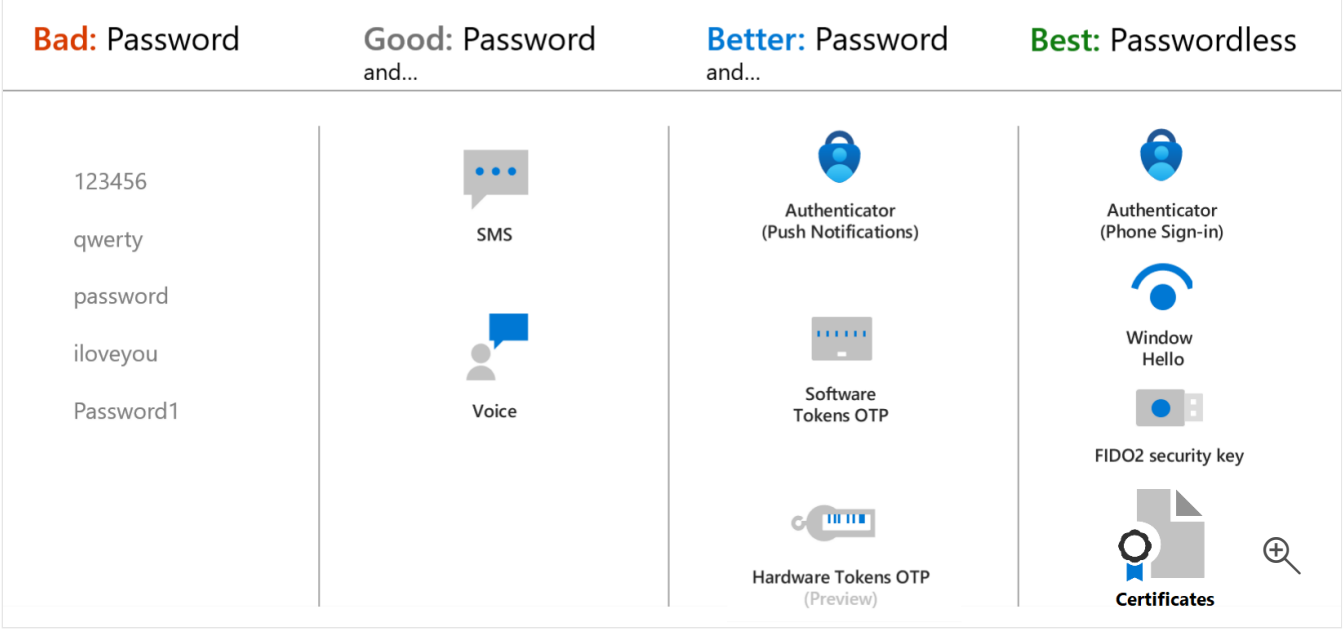
10 minutes

**One of the main features of an identity platform is to verify, or authenticate, credentials when a user signs in to a device, application, or service. Microsoft Entra ID offers different methods of authentication.**

## Passwords

**Passwords are the most common form of authentication, but they have many problems, especially if used in single-factor authentication, where only one form of authentication is used. If they're easy enough to remember, they're easy for a hacker to compromise. Strong passwords that aren't easily hacked are difficult to remember and affect user productivity when forgotten.**

**The use of passwords should be supplemented or replaced with more secure authentication methods available in Microsoft Entra ID.**




## Phone

**Microsoft Entra ID supports two options for phone-based authentication.**

- **SMS-based authentication. Short message service (SMS) used in mobile device text messaging can be used as a primary form of authentication. With SMS-based sign-**

in, users don't need to know a username and password to access applications and services. The user instead enters their registered mobile phone number, receives a text message with a verification code, and enters that in the sign-in interface.

Users can also choose to verify their identity through SMS text messaging on a mobile phone, as a secondary form of authentication during self-service password reset (SSPR) or Microsoft Entra Multifactor Authentication. For example, users can supplement their password by using SMS text messaging. An SMS is sent to the mobile phone number containing a verification code. To complete the sign-in process, the verification code provided is entered into the sign-in interface.

- Voice call verification. Users can use voice calls as a secondary form of authentication, to verify their identity, during self-service password reset (SSPR) or Microsoft Entra Multifactor Authentication. With phone call verification, an automated voice call is made to the phone number registered by the user. To complete the sign-in process, the user is prompted to press # on their keypad. Voice calls are not supported as a primary form of authentication, in Microsoft Entra ID.

## OATH

OATH (Open Authentication) is an open standard that specifies how time-based, one-time password (TOTP) codes are generated. One-time password codes can be used to authenticate a user. OATH TOTP is implemented using either software or hardware to generate the codes.

- Software OATH tokens are typically applications. Microsoft Entra ID generates the secret key, or seed, that's input into the app and used to generate each OTP.
- OATH TOTP hardware tokens (supported in public preview) are small hardware devices that look like a key fob that displays a code that refreshes every 30 or 60 seconds. OATH TOTP hardware tokens typically come with a secret key, or seed, preprogrammed in the token. These keys and other information specific to each token must be input into Microsoft Entra ID and then activated for use by end-users.

OATH software and hardware tokens, are only supported as secondary forms of authentication in Microsoft Entra ID, to verify an identity during self-service password reset (SSPR) or Microsoft Entra Multifactor Authentication.

## Passwordless authentication

**The end-goal for many organizations is to remove the use of passwords as part of sign-in events. When a user signs in with a passwordless method, credentials are provided by using methods like biometrics with Windows Hello for Business, or a FIDO2 security key. These authentication methods can't be easily duplicated by an attacker.**

**Microsoft Entra ID provides ways to natively authenticate using passwordless methods to simplify the sign-in experience for users and reduce the risk of attacks.**

**The following video explains the problem with passwords, and why passwordless authentication is so important.**

## Windows Hello for Business

**Windows Hello for Business replaces passwords with strong two-factor authentication on devices. This two-factor authentication is a combination of a key or certificate tied to a device and something that the person knows (a PIN) or something that the person is (biometrics). PIN entry and biometric gesture both trigger the use of the private key to cryptographically sign data that is sent to the identity provider. The identity provider verifies the user's identity and authenticates the user.**

**Windows Hello for Business helps protect against credential theft, because an attacker must have both the device and the biometric info or PIN, making it more difficult to gain access without the employee's knowledge.**

**As a passwordless authentication method, Windows Hello for Business serves as a primary form of authentication. In addition, Windows Hello for Business can be used as a secondary form of authentication to verify an identity during multifactor authentication.**

## FIDO2

**Fast Identity Online (FIDO) is an open standard for passwordless authentication. FIDO allows users and organizations to leverage the standard to sign in to their resources using an external security key or a platform key built into a device, eliminating the need for a username and password.**

**FIDO2 is the latest standard that incorporates the web authentication (WebAuthn) standard and is supported by Microsoft Entra ID. FIDO2 security keys are an unphishable standards-based passwordless authentication method that can come in any form factor. These FIDO2 security keys are typically USB devices, but could also be Bluetooth or Near Field Communication (NFC) based devices, which are used for short-range wireless data**

**transfer. With a hardware device that handles the authentication, the security of an account is increased as there's no password that could be exposed or guessed.**

**With FIDO2 security keys, users can sign in to Microsoft Entra ID or hybrid Microsoft Entra ID joined Windows 10 devices and get single-sign on to their cloud and on-premises resources. Users can also sign in to supported browsers. FIDO2 security keys are a great option for enterprises who are very security sensitive or have scenarios or employees who aren't willing or able to use their phone as a second factor.**

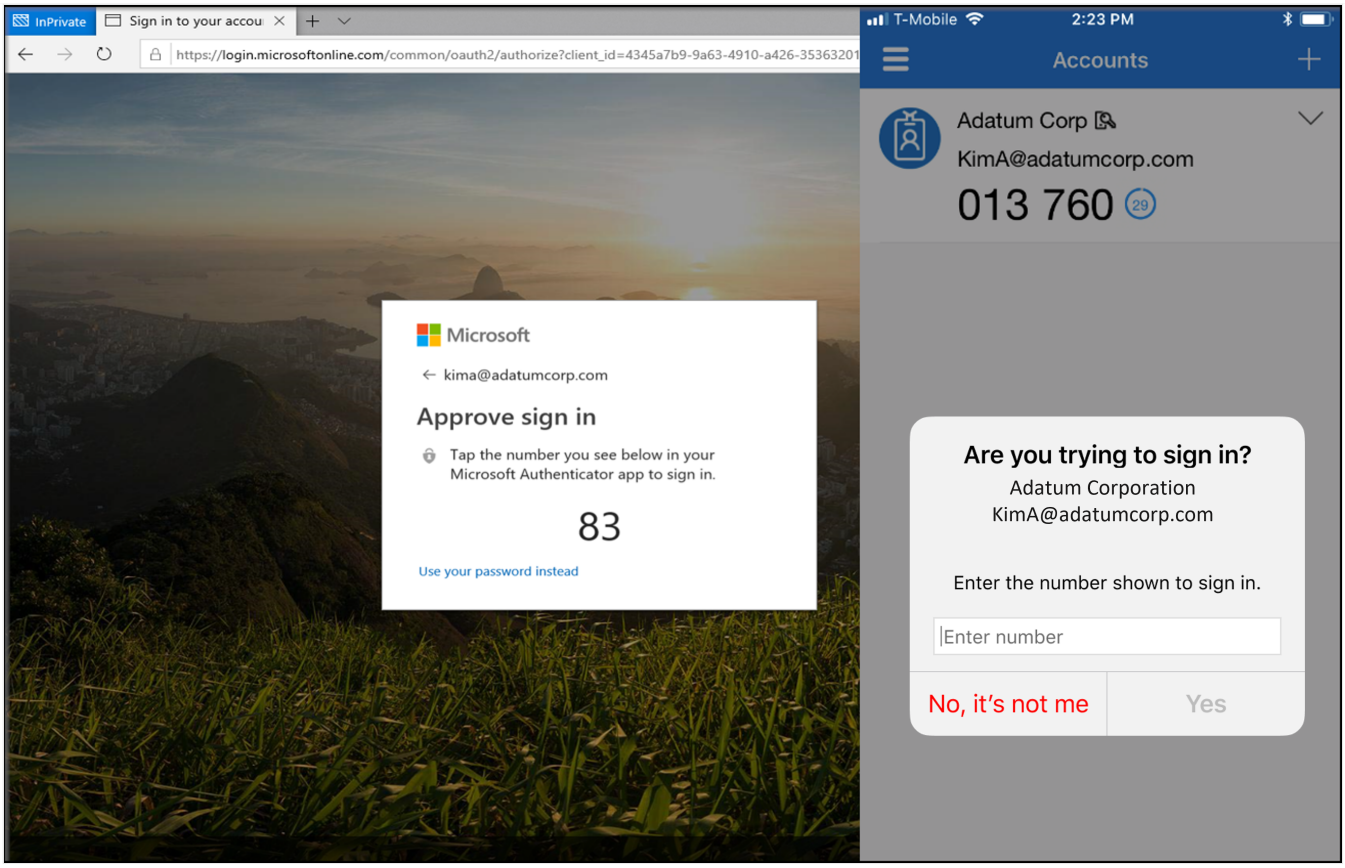
**As a passwordless authentication method, FIDO2 serves as a primary form of authentication. In addition, FIDO2 can be used as a secondary form of authentication to verify an identity during multifactor authentication.**

## Microsoft Authenticator app

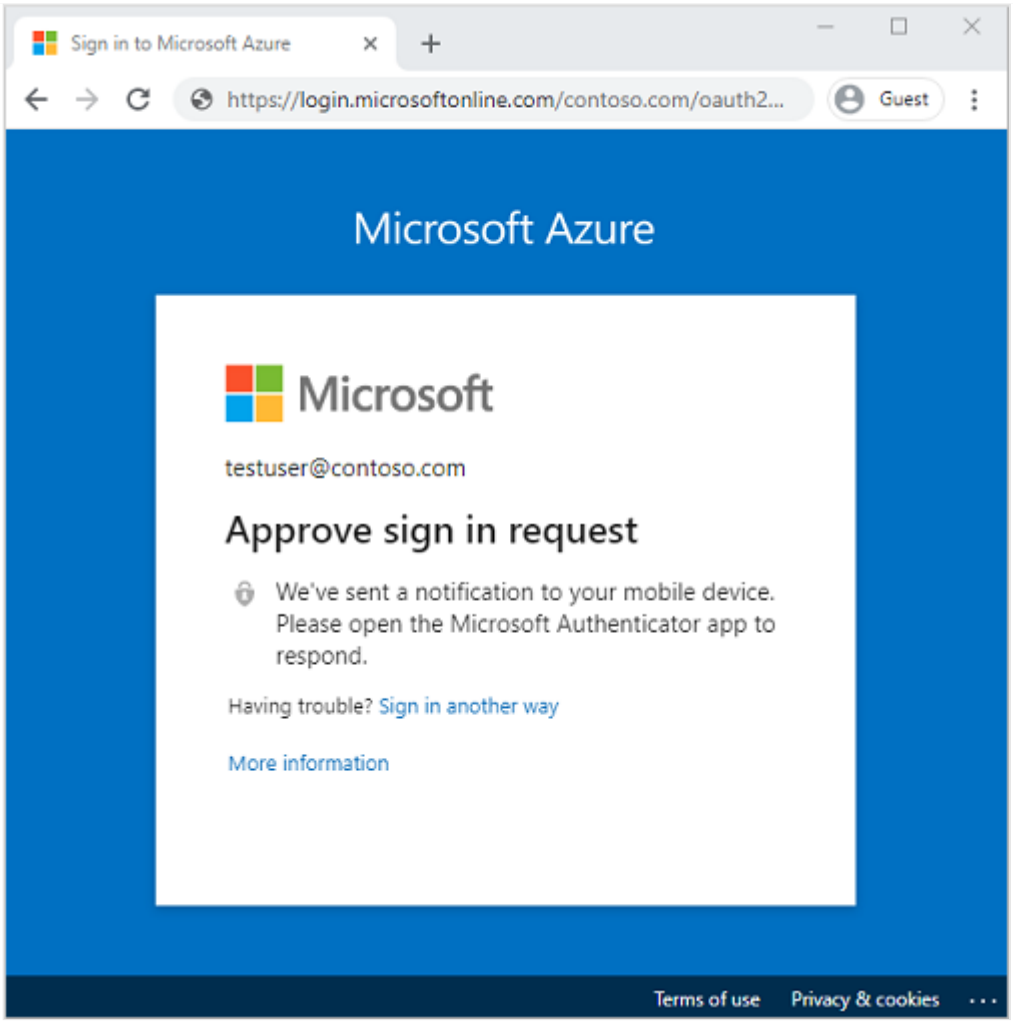
**As a passwordless authentication method, the Microsoft Authenticator app can be used as a primary form of authentication to sign in to any Microsoft Entra ID account or as an additional verification option during self-service password reset (SSPR) or Microsoft Entra Multifactor Authentication events.**

**To use Microsoft Authenticator, a user must download the phone app from the Microsoft store and register their account. Microsoft Authenticator is available for Android and iOS.**

**With Passwordless sign-in, the Authenticator App turns any iOS or Android phone into a strong, passwordless credential. To sign in to their Microsoft Entra ID account, a user enters their username, matches a number displayed on the screen to the one on their phone, then uses their biometric or PIN to confirm.**




**When a user chooses Authenticator as secondary form of authentication, to verify their identity, a notification is pushed to the phone or tablet. If the notification is legitimate, the user selects Approve, otherwise, they select Deny.**




**The Authenticator app can also be used as a software token to generate an OATH verification code. After entering your username and password, you enter the code provided by the Authenticator app into the sign-in interface. The OATH verification code provides a second form of authentication for SSPR or MFA.**

## Certificate-based authentication

**Microsoft Entra Identity certificate-based authentication (CBA) enables customers to allow or require users to authenticate directly with X.509 certificates against their Microsoft Entra Identity, for applications and browser sign-in. CBA is supported only as a primary form of passwordless authentication.**

**X.509 certificates, which are part of the public key infrastructure (PKI), are digitally signed documents that bind an identity (an individual, organization, website) to its public key. For more information, see Describe concepts of cryptography.**

## Primary and secondary authentication

**Some authentication methods can be used as the primary factor when you sign in to an application or device. Other authentication methods are only available as a secondary**

**factor when you use Microsoft Entra Multifactor Authentication or SSPR. While that information is called-out in the text that describes each authentication method, the following table summarizes when an authentication method can be used during a sign-in event.**

| Microsoft Entra Authentication Methods | | |
|---|---|---|
| **Method** | **Primary authentication** | **Secondary authentication** |
| Windows Hello for Business | Yes | MFA (users must be enabled for FIDO2) |
| Microsoft Authenticator | Yes | MFA and SSPR |
| FIDO2 security key | Yes | MFA |
| Certificate-based authentication | Yes | No |
| OATH hardware tokens (preview) | No | MFA and SSPR |
| OATH software tokens | No | MFA and SSPR |
| SMS | Yes | MFA and SSPR |
| Voice call | No | MFA and SSPR |
| Password | Yes | No |

## Next unit: Describe multifactor authentication

Continue >

**How are we doing?** ☆ ☆ ☆ ☆ ☆

100 XP

# Describe multifactor authentication

3 minutes

**Multifactor authentication is a process in which users are prompted during the sign-in process for an additional form of identification, such as a code on their cellphone or a fingerprint scan.**

**Multifactor authentication dramatically improves the security of an identity, while still being simple for users. The extra authentication factor must be something that's difficult for an attacker to obtain or duplicate.**

**Microsoft Entra multifactor Authentication works by requiring:**

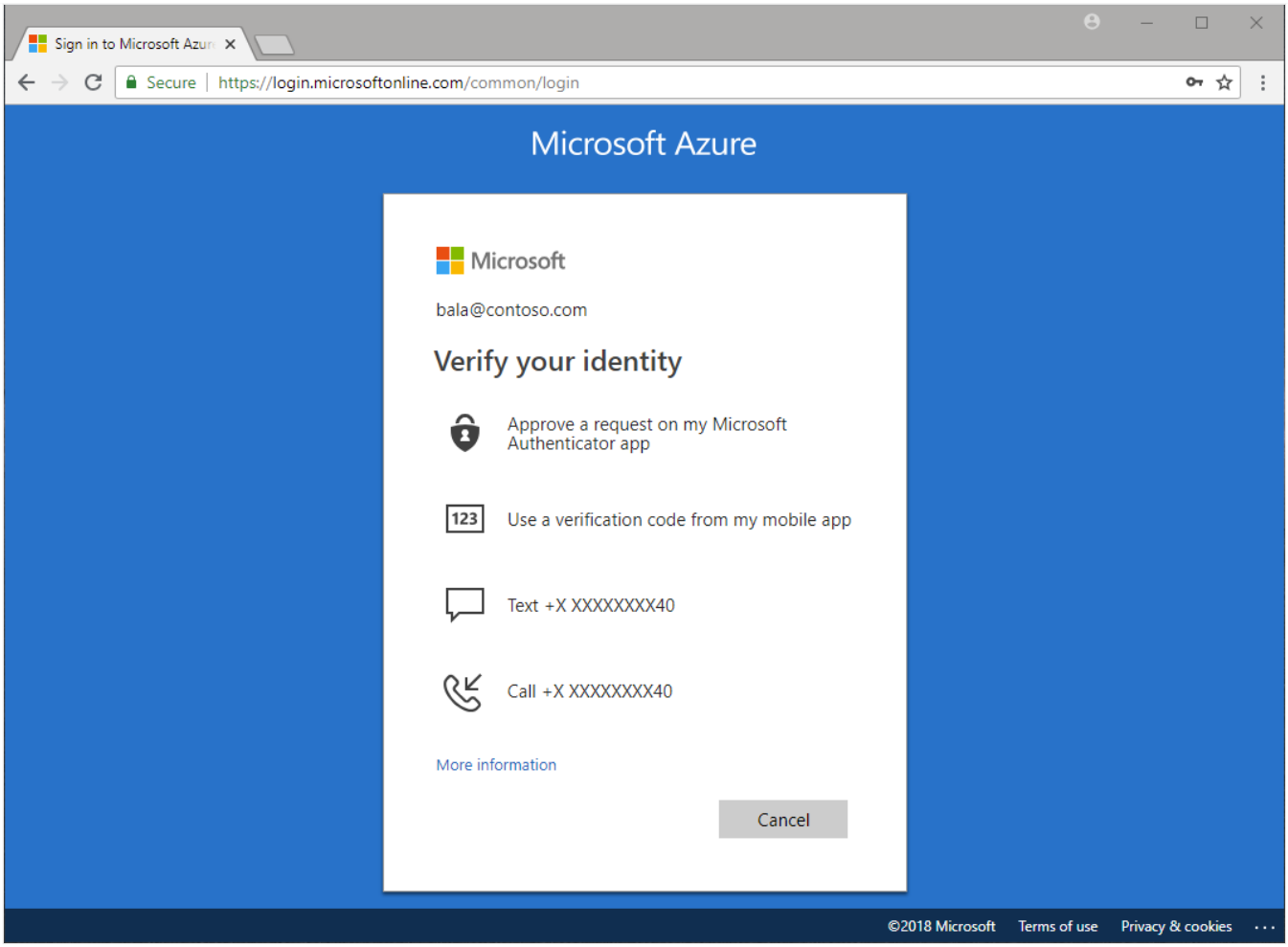
- **Something you know – typically a password or PIN and**
- **Something you have – such as a trusted device that's not easily duplicated, like a phone or hardware key or**
- **Something you are – biometrics like a fingerprint or face scan.**

**Multifactor authentication verification prompts are configured to be part of the Microsoft Entra ID sign-in event. Microsoft Entra ID automatically requests and processes multifactor authentication, without you making any changes to your applications or services. When a user signs in, they receive a multifactor authentication prompt, and can choose from one of the additional verification forms that they've registered.**

**An administrator can require certain verification methods, or the user can access their MyAccount to edit or add verification methods.**

**The following additional forms of verification, described in the previous unit, can be used with Microsoft Entra multifactor authentication:**

- **Microsoft Authenticator app**
- **Windows Hello for Business**
- **FIDO2 security key**
- **OATH hardware token (preview)**
- **OATH software token**
- **SMS**
- **Voice call**




## Security defaults and multifactor authentication

**Security defaults are a set of basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations are automatically enforced in your organization. The goal is to ensure that all organizations have a basic level of security enabled at no extra cost. These defaults enable some of the most common security features and controls, including:**

- **Enforcing Microsoft Entra multifactor authentication registration for all users.**
- **Forcing administrators to use multifactor authentication.**
- **Requiring all users to complete multifactor authentication when needed.**

**Security defaults are a great option for organizations that want to increase their security posture but don't know where to start, or for organizations using the free tier of Microsoft Entra ID licensing. Security defaults may not be appropriate for organizations with Microsoft Entra ID premium licenses or more complex security requirements. To learn more, visit What are security defaults?**

---

## Next unit: Describe self-service password reset

Continue >

**How are we doing?** ☆ ☆ ☆ ☆ ☆

100 XP

# Describe self-service password reset

6 minutes

**Self-service password reset (SSPR) is a feature of Microsoft Entra that allows users to change or reset their password, without administrator or help desk involvement. SSPR has several key benefits for organizations and users:**

- **SSPR reduces IT support costs by enabling users to reset passwords on their own.**
- **SSPR allows users to get back to work faster and be more productive.**
- **Administrators can change settings to accommodate new security requirements and roll these changes out to users without disrupting their sign-in.**
- **SSPR includes robust audit logs that are available from an API, enabling data to be imported to a Security Incident and Event Monitoring (SIEM) system of choice.**

**If a user's account is locked or they forget or want to change their password, they can follow a prompt to reset it and get back to work. This ability reduces help desk calls and loss of productivity when a user can't sign in to their device or an application.**

**To use self-service password reset, users must be:**

- **Assigned a Microsoft Entra ID license. Refer to the Learn More section of the summary and resources unit for a link to the Licensing requirements for Microsoft Entra self-service password reset.**
- **Enabled for SSPR by an administrator.**
- **Registered, with the authentication methods they want to use. Two or more authentication methods are recommended in case one is unavailable.**

**The following authentication methods are available for SSPR:**

- **Mobile app notification**
- **Mobile app code**
- **Email**
- **Mobile phone**
- **Office phone**
- **Security questions**

**When users register for SSPR, they're prompted to choose the authentication methods to use. If they choose to use security questions, they pick from a set of questions to prompt for, and then provide their own answers. Security questions can only be used during the self-service password reset (SSPR) process to confirm who you are, as a secondary form**

**of authentication. Security questions aren't used as an authentication method during a sign-in event. Administrator accounts can't use security questions as verification method with SSPR.**

> **Note**
>
> **By default, administrator accounts are enabled for self-service password reset and are required to use two authentication methods to reset their password, such as an email address, authenticator app, or a phone number. Administrators don't have the ability to use security questions.**

**When a user resets their password using self-service password reset, it can also be written back to an on-premises Active Directory. Password write-back allows users to use their updated credentials with on-premises devices and applications without a delay.**

**To keep users informed about account activity, admins can configure email notifications to be sent when an SSPR event happens. These notifications can cover both regular user accounts and admin accounts. For admin accounts, this notification provides an extra layer of awareness when a privileged administrator account password is reset using SSPR. All global admins would be notified when SSPR is used on an admin account.**

## Next unit: Describe password protection and management capabilities

Continue >

**How are we doing?** ☆ ☆ ☆ ☆ ☆

100 XP

# Describe password protection and management capabilities

4 minutes

**Password protection is a feature of Microsoft Entra that reduces the risk of users setting weak passwords. Microsoft Entra password protection detects and blocks known weak passwords and their variants, and can also block other weak terms that are specific to your organization.**

**With Microsoft Entra password protection, default global banned password lists are automatically applied to all users in a Microsoft Entra tenant. To support your own business and security needs, you can define entries in a custom banned password list. When users change or reset their passwords, these lists are checked to enforce the use of strong passwords.**

**You should use extra features like multifactor authentication, not just rely on strong passwords enforced by Microsoft Entra password protection.**

## Global banned password list

**A global banned password list with known weak passwords is automatically updated and enforced by Microsoft. This list is maintained by the Microsoft Entra ID Protection team, who analyzes security telemetry data to find weak or compromised passwords. Examples of passwords that might be blocked are P@$$w0rd or Passw0rd1 and all variations.**

**Variations are created using an algorithm that transposes text case and letters to numbers such as "1" to an "l". Variations on Password1 might include Passw0rd1, Pass0rd1, and others. These passwords are then checked and added to the global banned password list. The global banned password list is automatically applied to all users in a Microsoft Entra tenant and can't be disabled.**

**If a Microsoft Entra ID user tries to set their password to one of these weak passwords, they receive a notification to choose a more secure one. The global banned list is sourced from real-world, actual password spray attacks. This approach improves the overall security and effectiveness, and the password validation algorithm also uses smart fuzzy-matching techniques used to find strings that approximately match a pattern. Microsoft Entra password protection efficiently detects and blocks millions of the most common weak passwords from being used in your enterprise.**

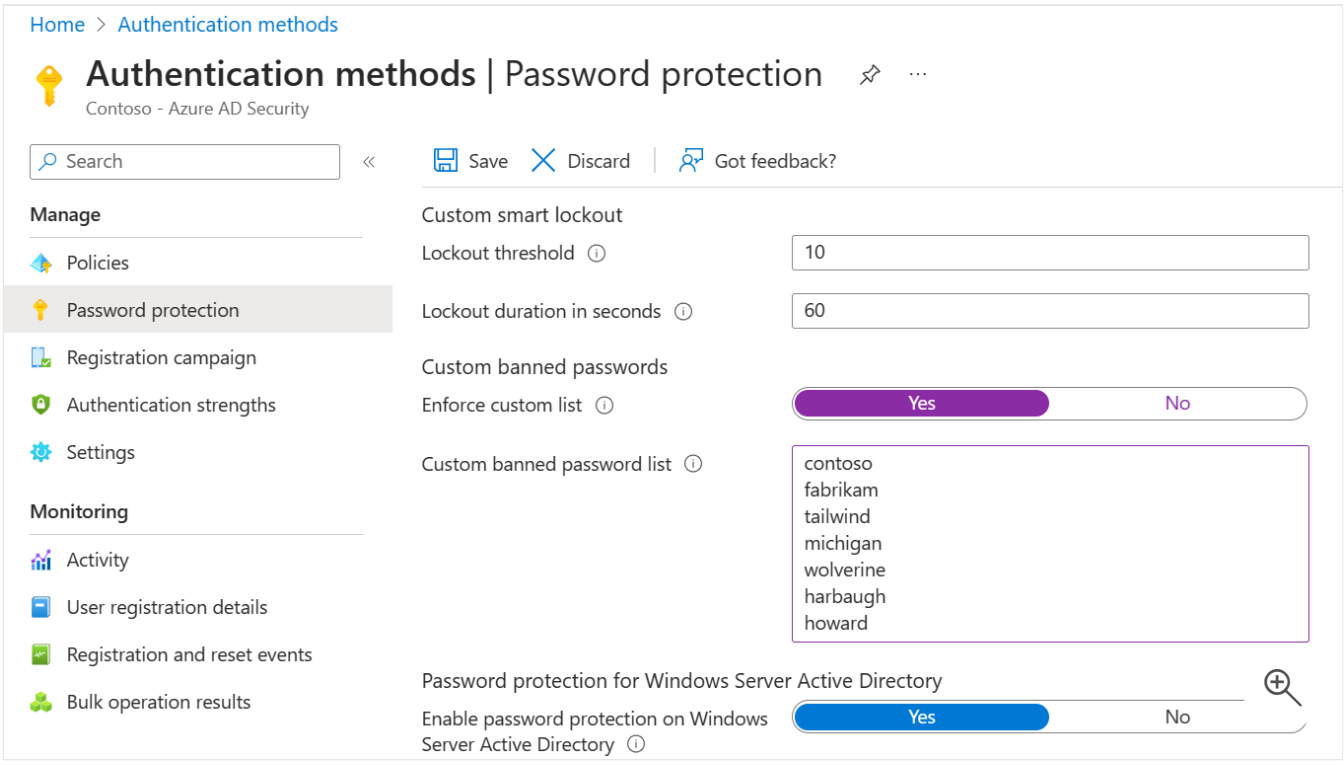
# Custom banned password lists

**Admins can also create custom banned password lists to support specific business security needs. The custom banned password list prohibits passwords such as the organization name or location. Passwords added to the custom banned password list should be focused on organizational-specific terms such as:**

- **Brand names**
- **Product names**
- **Locations, such as company headquarters**
- **Company-specific internal terms**
- **Abbreviations that have specific company meaning**

**The custom banned password list is combined with the global banned password list to block variations of all the passwords.**

**Banned password lists are a feature of Microsoft Entra ID premium licensing.**




# Protecting against password spray

**Microsoft Entra password protection helps you defend against password spray attacks. Most password spray attacks submit only a few of the known weakest passwords against each of the accounts in an enterprise. This technique allows the attacker to quickly search for an easily compromised account and avoid potential detection thresholds.**

**Microsoft Entra password protection efficiently blocks all known weak passwords likely to be used in password spray attacks. This protection is based on real-world security telemetry data from Microsoft Entra ID, which is used to build the global banned password list.**

## Hybrid security

**For hybrid security, admins can integrate Microsoft Entra password protection within an on-premises Active Directory environment. A component installed in the on-premises environment receives the global banned password list and custom password protection policies from Microsoft Entra ID. Domain controllers then use them to process password change events. This hybrid approach makes sure that, wherever a user changes their password, Microsoft Entra password protection is applied.**

**Although password protection improves the strength of passwords, you should still use best practice features like multifactor authentication. Passwords alone, even strong ones, are not as secure as multiple layers of security.**

---

## Next unit: Knowledge check

Continue >

---

**How are we doing?** ☆ ☆ ☆ ☆ ☆

100 XP

# Summary and resources

1 minute

**In this module, you've seen why passwords are a problematic form of authentication. You've learned about the different types of authentication that can be used with Microsoft Entra ID, including passwordless authentication with Windows Hello for Business and the Microsoft Authenticator app. You've learned about multifactor authentication.**

**You've learned about the benefits of allowing users to reset their own passwords with self-service password reset and how Microsoft Entra Password Protection mitigates against the inherent risks associated with passwords.**

**Now that you've completed this module, you can:**

- **Describe the authentication methods of Microsoft Entra ID.**
- **Describe multifactor authentication in Microsoft Entra ID**
- **Describe the password protection and management capabilities of Microsoft Entra ID.**

## Learn more

- What is Microsoft Entra ID Authentication?
- What authentication and verification methods are available in Microsoft Entra ID?
- Authentication methods in Microsoft Entra ID - Microsoft Authenticator app
- Authentication methods in Microsoft Entra ID - OATH tokens
- Passwordless authentication options for Microsoft Entra ID
- Authentication methods in Microsoft Entra ID - phone options
- FIDO2 security keys
- Windows Hello for Business
- How it works: Microsoft Entra ID multifactor authentication
- What are security defaults?
- Enable users to unlock their account or reset passwords using Microsoft Entra ID self-service password reset
- Eliminate bad passwords using Microsoft Entra ID Password Protection

## Module complete:

Continue to next module >

**How are we doing?** ☆ ☆ ☆ ☆ ☆

100 XP

# Introduction

1 minute

**The security perimeter has shifted away from organizational boundaries to user, device, and service identities. In this module, you'll learn how Microsoft Entra uses intelligent access management capabilities to protect organizational assets. This module describes how Conditional Access helps organization improve security. It also describes the purpose of Microsoft Entra roles and role-based access control, and how they're used to control access to Microsoft Entra resources.**

**In this module, you'll learn how to:**

- **Describe Conditional Access in Microsoft Entra.**
- **Describe Microsoft Entra roles and role-based access control.**

## Next unit: Describe Conditional Access

Continue

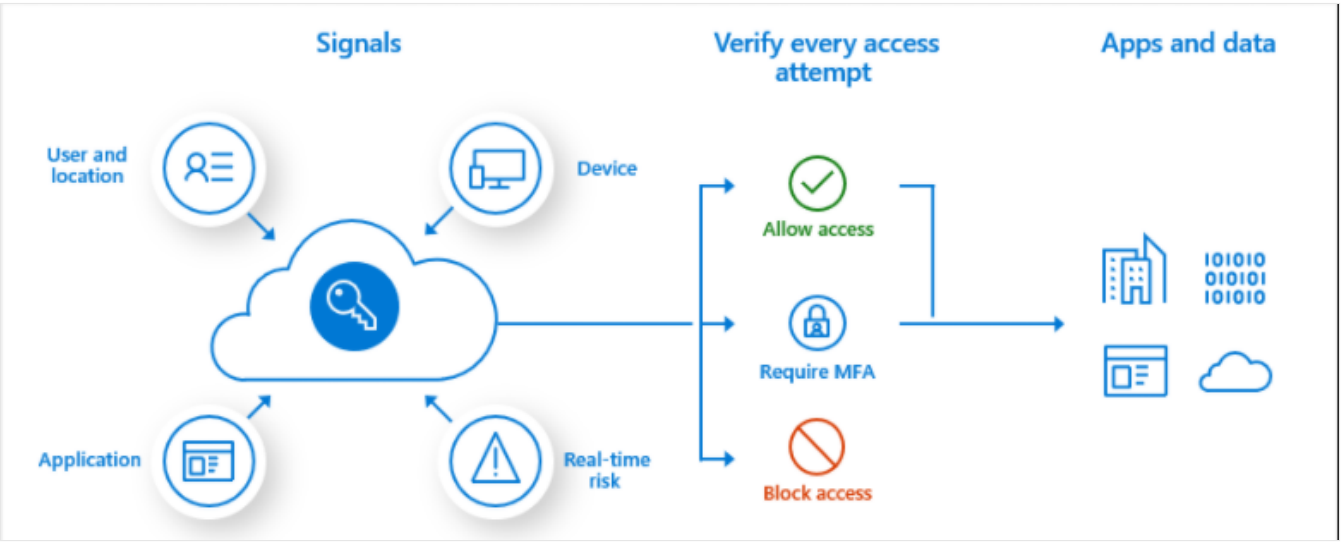
**How are we doing?** ☆ ☆ ☆ ☆ ☆

100 XP

# Describe Conditional Access

9 minutes

**Conditional Access is a feature of Microsoft Entra that provides an extra layer of security before allowing authenticated users to access data or other assets. Conditional Access is implemented through policies that are created and managed in Microsoft Entra ID. A Conditional Access policy analyses signals including user, location, device, application, and risk to automate decisions for authorizing access to resources (apps and data).**



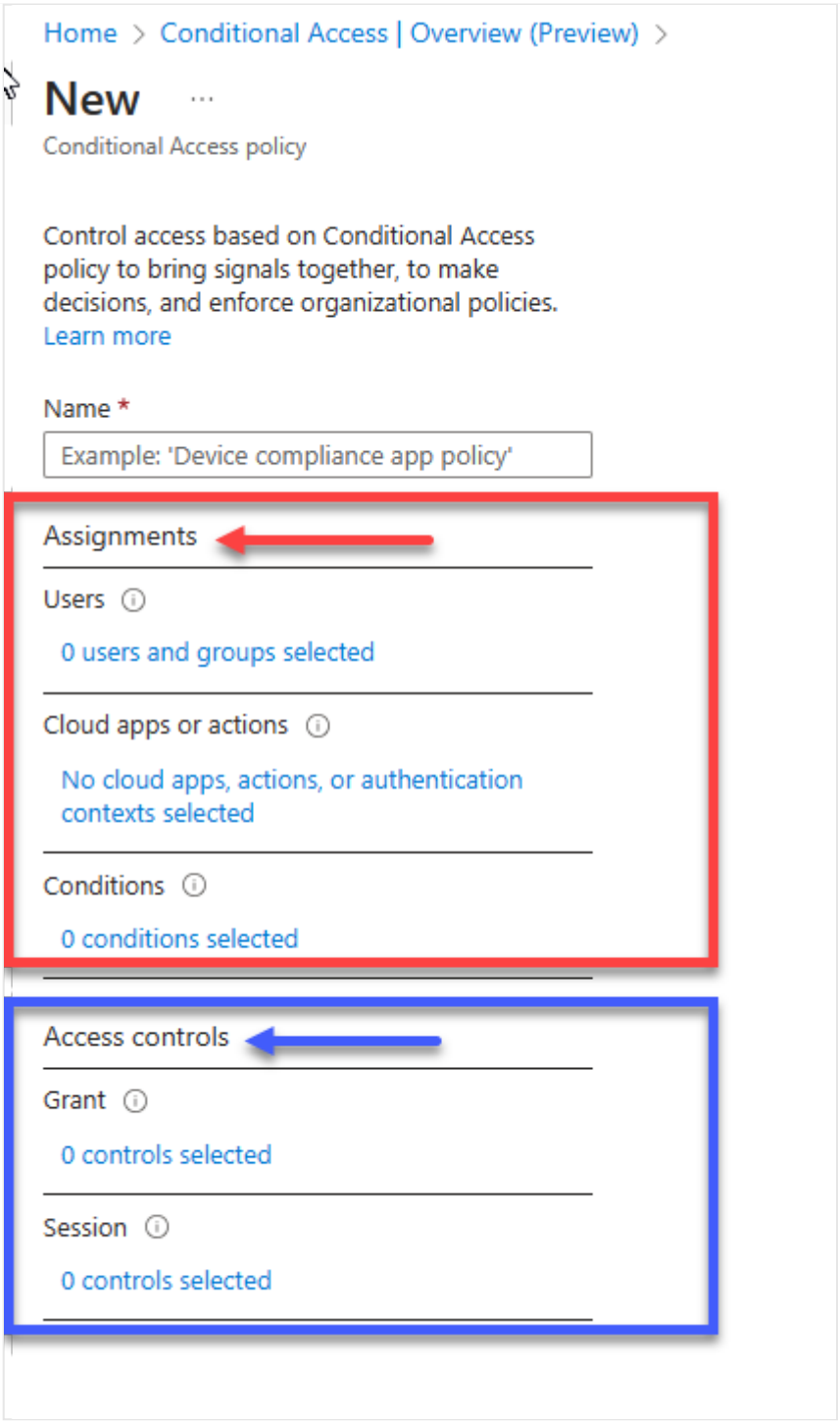

**Conditional Access policies at their simplest are if-then statements. For example, a Conditional Access policy might state that *if* a user belongs to a certain group, then they're required to provide multi-factor authentication to sign in to an application.**

> **ⓘ Important**
>
> **Conditional Access policies are enforced after first-factor authentication is completed. Conditional Access isn't intended to be an organization's first line of defense for scenarios like denial-of-service (DoS) attacks, but it can use signals from these events to determine access.**

**Watch the video to see how Conditional Access policies work.**

## Conditional access policy components

**A conditional access policy in Microsoft Entra ID consists of two components, assignments and access controls.**




## Assignments

**When creating a conditional access policy, admins can determine which signals to use through assignments. The assignments portion of the policy controls the who, what, where, and when of the Conditional Access policy. All assignments are logically ANDed. If you have more than one assignment configured, all assignments must be satisfied to trigger a policy. Some of the assignments include:**

- **Users and groups assign who the policy will include or exclude. This assignment can include all users, specific groups of users, directory roles, or external guest users.**

**This assignment can also include single tenant service principals (applications) that are registered in your tenant.**

- **Cloud apps or actions can include or exclude cloud applications, user actions, or authentication contexts that are subjected to the policy. Integration of Microsoft Defender for Cloud with conditional access enables real-time visibility and control over access to and activities performed within your cloud environment.**
- **Conditions define where and when the policy will apply. Multiple conditions can be combined to create fine-grained and specific Conditional Access policies. Some of the conditions include:**
  - **Sign-in risk and user risk. Integration with Microsoft Entra ID Protection allows Conditional Access policies to identify suspicious actions related to user accounts in the directory and trigger a policy. Sign-in risk is the probability that a given sign-in, or authentication request, isn't authorized by the identity owner. User risk is the probability that a given identity or account is compromised.**
  - **Devices platform. Device platform, which is characterized by the operating system that runs on a device can be used when enforcing Conditional Access policies.**
  - **IP location information. Organizations can define trusted IP address ranges that can be used when making policy decisions. Also, administrators can opt to block or allow traffic from an entire country/region's IP range.**
  - **Client apps. Clients apps, the software the user is employing to access the cloud app, including browsers, mobile apps, desktop clients, can also be used in access policy decision.**
  - **Filters for devices. Organizations can enforce policies based on device properties, by using the filters for devices option. As an example, this option may be used to target policies to specific devices like privileged access workstations.**

## Access controls

**When the Conditional Access policy has been applied, an informed decision is reached on whether to block access, grant access, grant access with extra verification, or apply a session control to enable a limited experience. The decision is referred to as the access controls portion of the Conditional Access policy and defines how a policy is enforced. Common decisions are:**

- **Block access**
- **Grant access. Administrators can grant access without any additional control, or they can choose to enforce one or more controls when granting access. Examples of controls used to grant access include requiring users to perform multifactor authentication, requiring specific authentication methods to access a resource, requiring devices to meet specific compliance policy requirements, require a**

password change, and more. For a complete list, refer to Grant controls in Conditional Access policy.

- Session. Within a Conditional Access policy, an administrator can make use of session controls to enable limited experiences within specific cloud applications. As an example, Conditional Access App Control uses signals from Microsoft Defender for Cloud Apps to block the download, cut, copy, and print capabilities for sensitive documents, or to require labeling of sensitive files. Other session controls include sign-in frequency and application enforced restrictions that, for selected applications, use the device information to provide users with a limited or full experience, depending on the device state. For a complete list, refer Session controls in Conditional Access policy.

## Interactive Guide

In this interactive guide, you'll walk through the different assignments and access controls for a conditional access policy and then create a Conditional Access policy for a group of users.


## Next unit: Describe Microsoft Entra roles and role-based access control (RBAC)

Continue >

**How are we doing?** ☆ ☆ ☆ ☆ ☆

100 XP

# Describe Microsoft Entra roles and role-based access control (RBAC)

7 minutes

**Microsoft Entra roles control permissions to manage Microsoft Entra resources. For example, allowing user accounts to be created, or billing information to be viewed. Microsoft Entra supports built-in and custom roles.**

**Managing access using roles is known as role-based access control (RBAC). Microsoft Entra built-in and custom roles are a form of RBAC in that Microsoft Entra roles control access to Microsoft Entra resources. This is referred to as Microsoft Entra RBAC.**

## Built-in roles

**Microsoft Entra includes many built-in roles, which are roles with a fixed set of permissions. A few of the most common built-in roles are:**

- ***Global administrator*: users with this role have access to all administrative features in Microsoft Entra. The person who signs up for the Microsoft Entra tenant automatically becomes a global administrator.**
- ***User administrator*: users with this role can create and manage all aspects of users and groups. This role also includes the ability to manage support tickets and monitor service health.**
- ***Billing administrator*: users with this role make purchases, manage subscriptions and support tickets, and monitor service health.**

**All built-in roles are preconfigured bundles of permissions designed for specific tasks. The fixed set of permissions included in the built-in roles can't be modified.**

## Custom roles

**Although there are many built-in admin roles in Microsoft Entra, custom roles give flexibility when granting access. A custom role definition is a collection of permissions that you choose from a preset list. The list of permissions to choose from are the same permissions used by the built-in roles. The difference is that you get to choose which permissions you want to include in a custom role.**

**Granting permission using custom Microsoft Entra roles is a two-step process. The first step involves creating a custom role definition, consisting of a collection of permissions that you add from a preset list. Once you've created your custom role definition, the second step is to assign that role to users or groups by creating a role assignment.**

**A role assignment grants the user the permissions in a role definition, at a specified scope. A scope defines the set of Microsoft Entra ID resources the role member has access to. A custom role can be assigned at organization-wide scope, meaning the role member has the role permissions over all resources. A custom role can also be assigned at an object scope. An example of an object scope would be a single application. The same role can be assigned to one user over all applications in the organization and then to another user with a scope of only the Contoso Expense Reports app.**

**Custom roles require an Microsoft Entra ID premium license.**

## Only grant the access users need

**It's best practice, and more secure, to grant users the least privilege to get their work done. It means that if someone mostly manages users, you should assign the user administrator role, and not global administrator. By assigning least privileges, you limit the damage that could be done with a compromised account.**

## Categories of Microsoft Entra roles

**Microsoft Entra ID is an available service if you subscribe to any Microsoft Online business offer, such as Microsoft 365 and Azure.**

**Available Microsoft 365 services include Microsoft Entra ID, Exchange, SharePoint, Microsoft Defender, Teams, Intune, and many more.**

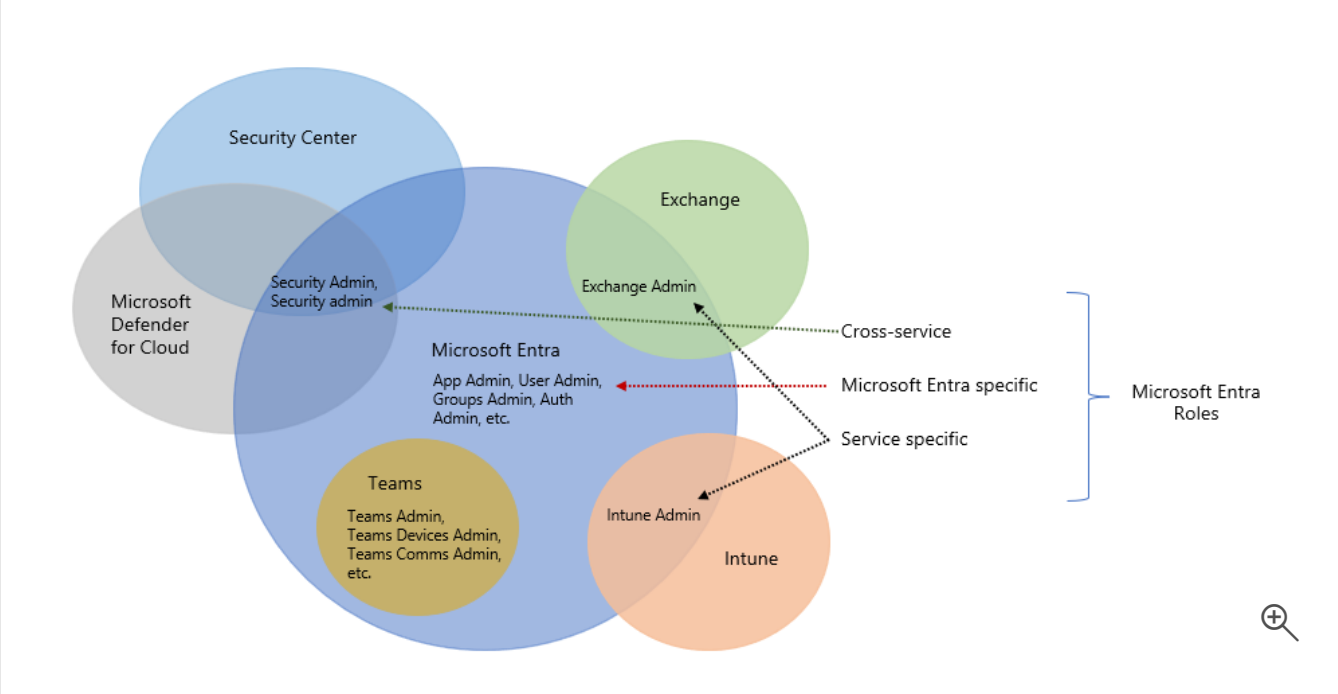
**Over time, some Microsoft 365 services, such as Exchange and Intune, have developed their own role-based access control systems (RBAC), just like the Microsoft Entra ID service has Microsoft Entra roles to control access to Microsoft Entra resources. Other services such as Teams and SharePoint don't have separate role-based access control systems, they use Microsoft Entra roles for their administrative access.**

**To make it convenient to manage identity across Microsoft 365 services, Microsoft Entra has added some service-specific, built-in roles, each of which grants administrative access to a Microsoft 365 service. This means that Microsoft Entra built-in roles differ in where they can be used. There are three broad categories.**

- **Microsoft Entra specific roles: These roles grant permissions to manage resources within Microsoft Entra ID only. For example, User Administrator, Application**

**Administrator, Groups Administrator all grant permissions to manage resources that live in Microsoft Entra ID.**

- **Service-specific roles: For major Microsoft 365 services, Microsoft Entra includes built-in, service-specific roles that grant permissions to manage features within the service. For example, Microsoft Entra includes built-in roles for Exchange Administrator, Intune Administrator, SharePoint Administrator, and Teams Administrator roles that can manage features with their respective services.**
- **Cross-service roles: There are some roles within Microsoft Entra that span services. For example, Microsoft Entra has security-related roles, like Security Administrator, that grant access across multiple security services within Microsoft 365. Similarly, the Compliance Administrator role grants access to manage Compliance-related settings in Microsoft 365 Compliance Center, Exchange, and so on.**




# Difference between Microsoft Entra RBAC and Azure RBAC

**As described above, Microsoft Entra built-in and custom roles are a form of RBAC in that they control access to Microsoft Entra resources. This is referred to as Microsoft Entra RBAC. In the same way that Microsoft Entra roles can control access to Microsoft Entra resources, so too can Azure roles control access to Azure resources. This is referred to as Azure RBAC. Although the concept of RBAC applies to both Microsoft Entra RBAC and Azure RBAC, what they control are different.**

- **Microsoft Entra RBAC - Microsoft Entra roles control access to Microsoft Entra resources such as users, groups, and applications.**

- **Azure RBAC - Azure roles control access to Azure resources such as virtual machines or storage using Azure Resource Management.**

**There are different data stores where role definitions and role assignments are stored. Similarly, there are different policy decision points where access checks happen.**

## Next unit: Knowledge check

Continue >

**How are we doing?** ☆ ☆ ☆ ☆ ☆

Previous Unit 5 of 5

100 XP

# Summary & resources

1 minute

**In this module, you've learned about Conditional Access and how it's used to protect resources. You've seen how Conditional Access policies use *if then* statements with signals to determine whether to grant access, require more information, or block access.**

**You also learned about built-in and custom roles in Microsoft Entra ID and how these are used to provide role-based access control.**

**Now that you've completed this module, you'll be able to:**

- **Describe Conditional Access in Microsoft Entra ID.**
- **Describe Microsoft Entra ID roles and role-based access control.**

## Learn more

**For more information about the topics raised in this module, see:**

- Conditional Access
- Security defaults
- Understand Azure Microsoft Entra ID role concepts
- Overview of role-based access control in Microsoft Entra ID
- Understand roles in Microsoft Entra ID
- Available roles

## Explore other modules

Microsoft Security, Compliance, and Identity Fundamentals: Describe the capabilities of Microsoft Entra
MS-900 Microsoft 365 Fundamentals: Describe Microsoft 365 security and compliance capabilities

**How are we doing?** ☆ ☆ ☆ ☆ ☆

100 XP

# Introduction

1 minute

**Identity governance is about balancing identity security with user productivity in a way that can be justified and audited. Identity protection is about protecting an organization's identities against risk and potential vulnerabilities.**

**Microsoft Entra provides many identity protection and governance capabilities that work together to mitigate risk by protecting, monitoring, and auditing access to critical assets while ensuring employee and business partner productivity.**

**In this module, you'll learn how to:**

- **Describe the identity governance capabilities of Microsoft Entra.**
- **Describe Privileged Identity Management (PIM).**
- **Describe the capabilities of Microsoft Entra ID Protection.**
- **Describe permissions management.**

## Next unit: Describe Microsoft Entra ID Governance

Continue

**How are we doing?** ☆ ☆ ☆ ☆ ☆

100 XP

# Describe Microsoft Entra ID Governance

4 minutes

**Microsoft Entra ID Governance allows you to balance your organization's need for security and employee productivity with the right processes and visibility. It provides you with capabilities to ensure that the right people have the right access to the right resources.**

**ID Governance gives organizations the ability to do the following tasks:**

- **Govern the identity lifecycle.**
- **Govern access lifecycle.**
- **Secure privileged access for administration.**

**These actions can be completed for employees, business partners and vendors, and across services and applications, both on-premises and in the cloud.**

**It's intended to help organizations address these four key questions:**

- **Which users should have access to which resources?**
- **What are those users doing with that access?**
- **Are there effective organizational controls for managing access?**
- **Can auditors verify that the controls are working?**

## Identity lifecycle

**Managing users' identity lifecycle is at the heart of identity governance.**

**When planning identity lifecycle management for employees, for example, many organizations model the "join, move, and leave" process. When an individual first joins an organization, a new digital identity is created if one isn't already available. When an individual moves between organizational boundaries, more access authorizations may need to be added or removed to their digital identity. When an individual leaves, access may need to be removed, and the identity might no longer be required, other than for audit purposes.**

**The diagram that follows shows a simplified version of the identity lifecycle.**


**For many organizations, this identity lifecycle for employees is tied to the representation of that user in a human resources (HR) system such as Workday or SuccessFactors. The HR system is authoritative for providing the current list of employees, and some of their properties, such as name or department.**

**Microsoft Entra Premium offers integration with cloud-based HR systems. When a new employee is added to an HR system, Microsoft Entra ID can create a corresponding user account. Similarly, when their properties, such as department or employment status, change in the HR system, synchronization of those updates to Microsoft Entra ID ensures consistency.**

**Microsoft Entra Premium also includes Microsoft Identity Manager, which can import records from on-premises HR systems such as SAP HCM, Oracle eBusiness, and Oracle PeopleSoft. For more information, see the Microsoft Identity Manager documentation that is listed in the Learn More section of the Summary and resources unit.**

**In general, managing the lifecycle of an identity is about updating the access that users need, whether through integration with an HR system, or through user provisioning applications.**

## Access lifecycle

**Access lifecycle is the process of managing access throughout the user's organizational life. Users require different levels of access from the point at which they join an organization to when they leave it. At various stages in between, they'll need access rights to different resources depending on their role and responsibilities.**

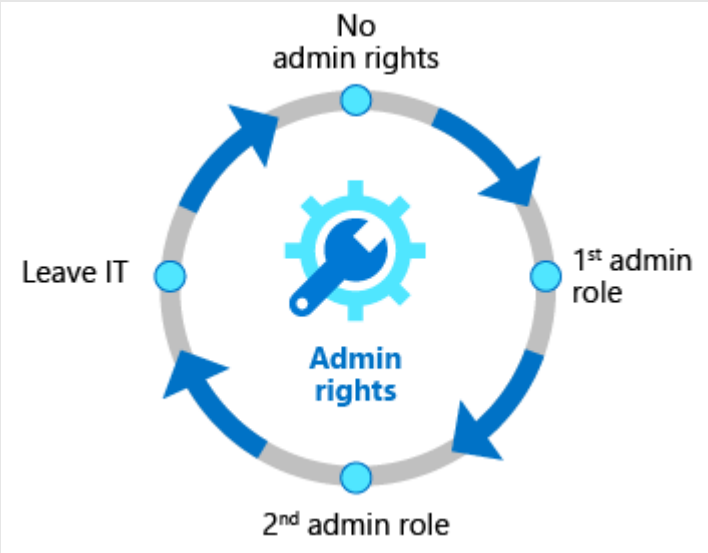
**Organizations can automate the access lifecycle process through technologies such as dynamic groups. Dynamic groups enable admins to create attribute-based rules to determine membership of groups. When any attributes of a user or device change, the**

**system evaluates all dynamic group rules in a directory to see if the change would trigger any users to be added or removed from a group. If a user or device satisfies a rule for a group, they're added as a member of that group. If they no longer satisfy the rule, they're removed.**

## Privileged access lifecycle

**Monitoring privileged access is a key part of identity governance. When employees, vendors, and contractors are assigned administrative rights, there should be a governance process because of the potential for misuse.**

**Microsoft Entra Privileged Identity Management (PIM) provides extra controls tailored to securing access rights. PIM helps you minimize the number of people who have access to resources across Microsoft Entra ID, Azure, and other Microsoft online services. PIM provides a comprehensive set of governance controls to help secure your company's resources.**




## Next unit: Describe access reviews

Continue >

**How are we doing?** ☆ ☆ ☆ ☆ ☆

100 XP

# Describe access reviews

8 minutes

**Microsoft Entra access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignment. Regular access reviews ensure that only the right people have access to resources. Excessive access rights are a known security risk. However, when people move between teams, or take on or relinquish responsibilities, access rights can be difficult to control.**

**Microsoft Entra enables you to collaborate with users from inside your organization and with external users. Users can join groups, invite guests, connect to cloud apps, and work remotely from their work or personal devices. This convenience has led to a need for better access management capabilities.**

**There are many use cases in which access reviews should be used, here are just a few examples.**

- **Too many users in privileged roles: It's a good idea to check how many users have administrative access and if there are any invited guests or partners that haven't been removed after being assigned to do an administrative task. You can recertify the role assignment of users in Microsoft Entra roles such as Global Administrators, or Azure resources roles such as User Access Administrator in the Microsoft Entra Privileged Identity Management (PIM) experience.**
- **Business critical data access: For certain resources, such as business critical applications, it might be required as part of compliance processes to ask people to regularly reconfirm and give a justification on why they need continued access.**
- **To maintain a policy's exception list: Sometimes there are business cases that require you to make exceptions to policies. As the IT admin, you can manage this task and provide auditors with proof that these exceptions are reviewed regularly.**
- **Ask group owners to confirm they still need guests in their groups: If a group gives guests access to business sensitive content, then it's the group owner's responsibility to confirm the guests still have a legitimate business need for access.**
- **Have reviews recur periodically: You can set up recurring access reviews of users at set frequencies such as weekly, monthly, quarterly or annually, and the reviewers will be notified at the start of each review. Reviewers can approve or deny access with a friendly interface and with the help of smart recommendations.**

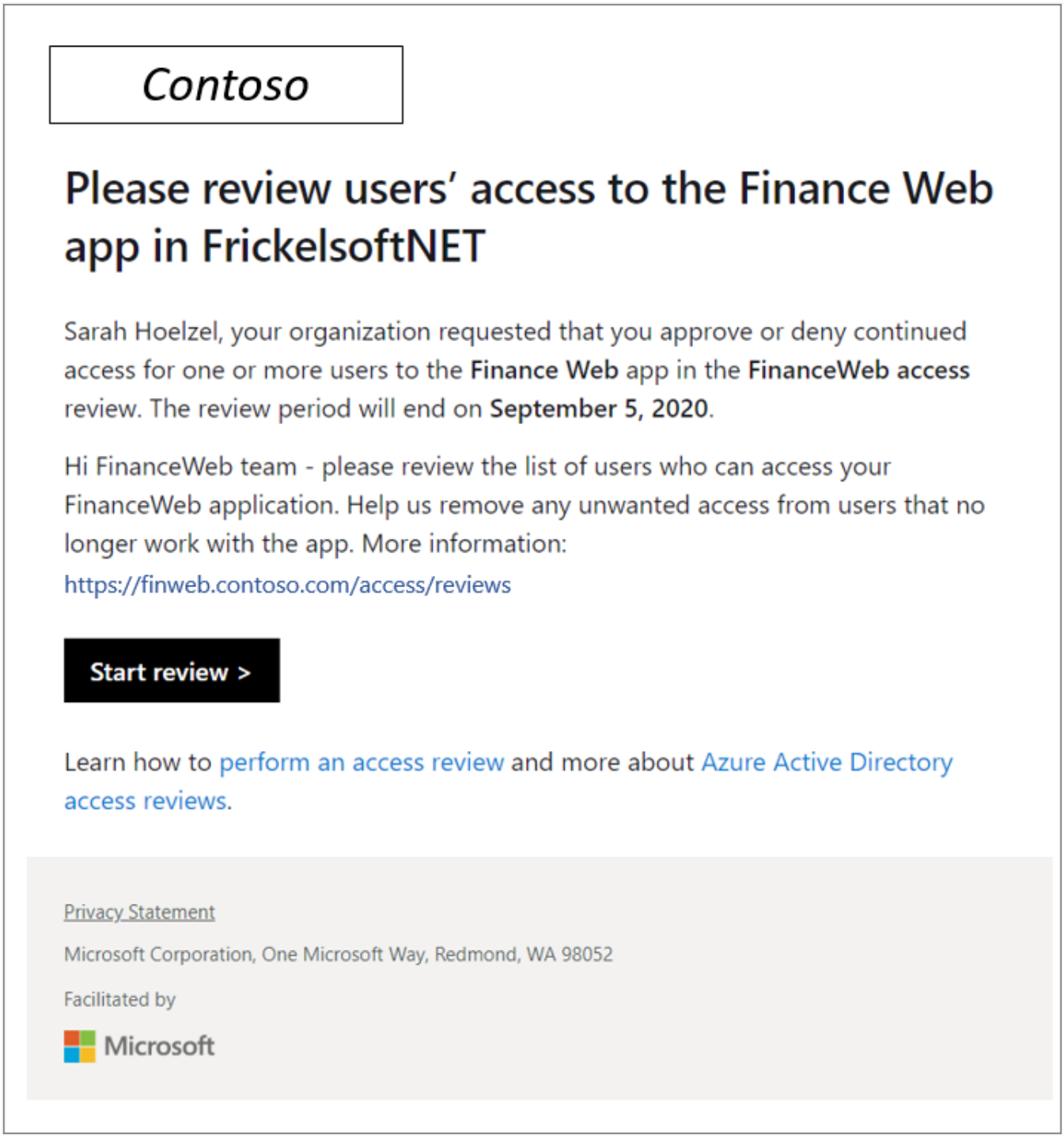
## Manage user and guest user access with access reviews

**With access reviews, you can easily ensure that users or guests have appropriate access. You can ask the users themselves or a decision maker to participate in an access review and recertify (or attest) to users' access. The reviewers can give their input on each user's need for continued access based on suggestions from Microsoft Entra ID. When an access review is finished, you can then make changes and remove access from users who no longer need it.**

## Multi-stage access reviews

**Microsoft Entra Access Reviews support up to three review stages, in which multiple types of reviewers engage in determining who still needs access to company resources. These reviews could be for membership in groups or teams, access to applications, assignments to privileged roles, or access package assignments. When review administrators configure the review for automatic application of decisions, at the end of the review period, access is revoked for denied users.**

**Multi-stage access reviews allow you and your organization to enable complex workflows to meet recertification and audit requirements calling for multiple reviewers to attest to access for users in a particular sequence. It also helps you design more efficient reviews for your resource owners and auditors by reducing the number of decisions each reviewer is accountable for.**




**Admins who create access reviews can track progress as the reviewers complete their process. No access rights are changed until the review is finished. You can, however, stop a review before it reaches its scheduled end.**

**When the review is complete, it can be set to manually or auto-apply changes to remove access from a group membership or application assignment, except for a dynamic group or a group that originates on-premises. In those cases, the changes must be applied directly to the group.**

---

## Next unit: Describe entitlement management

Continue >

**How are we doing?** ☆ ☆ ☆ ☆ ☆

100 XP

# Describe entitlement management

8 minutes

**Entitlement management is an identity governance feature that enables organizations to manage the identity and access lifecycle at scale. Entitlement management automates access request workflows, access assignments, reviews, and expiration.**

- **Users may not know what access they should have, and even if they do, they might have difficulty locating the right individuals to approve it.**
- **When users find and receive access to a resource, they may hold on to access longer than is required for business purposes.**
- **Managing access for external users.**

**Entitlement management includes the following capabilities to address these challenges:**

- **Delegate the creation of access packages to non-administrators. These access packages contain resources that users can request. The delegated access package managers then define policies that include rules such as which users can request access, who must approve their access, and when access expires.**
- **Managing external users. When a user who isn't yet in your directory requests access, and is approved, they're automatically invited into your directory and assigned access. When their access expires, if they have no other access package assignments, their B2B account in your directory can be automatically removed.**

**Entitlement management uses access packages to manage access to resources.**

## Microsoft Entra terms of use

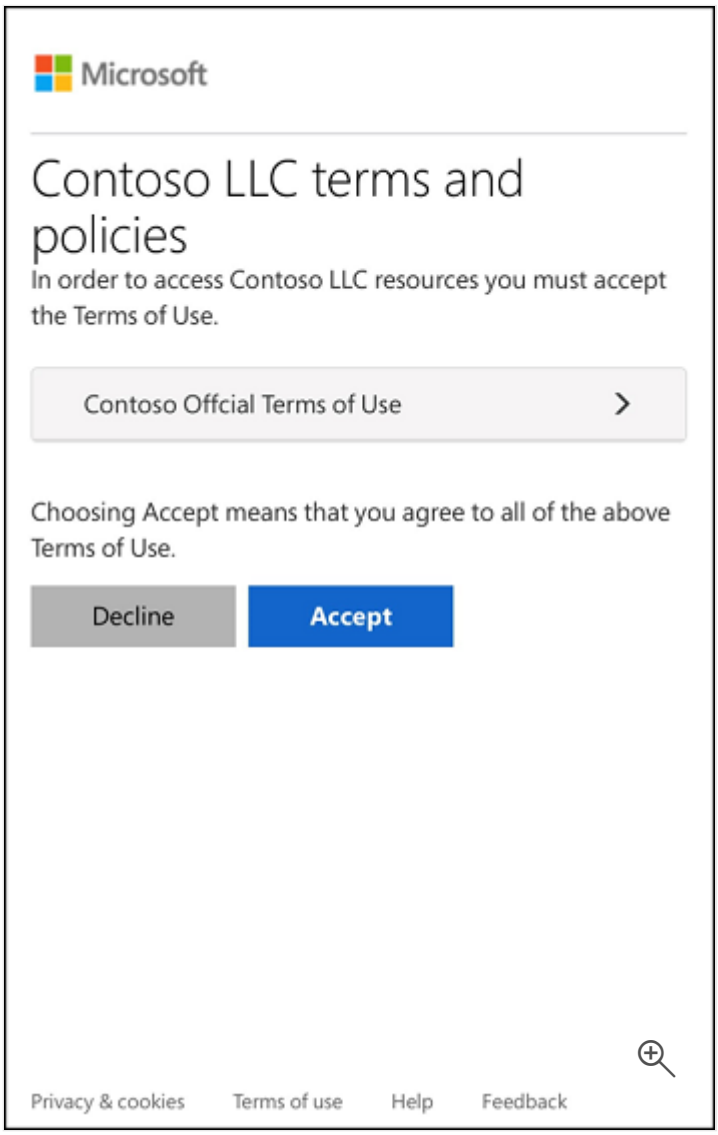
**Microsoft Entra terms of use allow information to be presented to users, before they access data or an application. Terms of use ensure users read relevant disclaimers for legal or compliance requirements.**

**Example use cases where employees or guests may be required to accept terms of use include:**

- **Before they access sensitive data or an application.**
- **On a recurring schedule, so they're reminded of regulations.**
- **Based on user attributes, such as terms applicable to certain roles.**
- **Presenting terms for all users in your organization.**

**Terms of use are presented in a PDF format, using content that you create, such as an existing contract document. Terms of use can also be presented to users on mobile devices.**

**Conditional Access policies are used to require a terms of use statement being displayed, and ensuring the user has agreed to those terms before accessing an application. Admins can then view who has agreed to terms of use, and who has declined.**




## Next unit: Describe the capabilities of Privileged identity Management

Continue

**How are we doing?** ☆ ☆ ☆ ☆ ☆

100 XP

# Describe the capabilities of Privileged identity Management

8 minutes

**Privileged Identity Management (PIM) is a service of Microsoft Entra that enables you to manage, control, and monitor access to important resources in your organization. These include resources in Microsoft Entra, Azure, and other Microsoft online services such as Microsoft 365 or Microsoft Intune. PIM mitigates the risks of excessive, unnecessary, or misused access permissions. It requires justification to understand why users want permissions, and enforces multifactor authentication to activate any role.**

**PIM is:**

- **Just in time, providing privileged access only when needed, and not before.**
- **Time-bound, by assigning start and end dates that indicate when a user can access resources.**
- **Approval-based, requiring specific approval to activate privileges.**
- **Visible, sending notifications when privileged roles are activated.**
- **Auditable, allowing a full access history to be downloaded.**

## Why use PIM?

**PIM reduces the chance of a malicious actor getting access by minimizing the number of people who have access to secure information or resources. By time-limiting authorized users, it reduces the risk of an authorized user inadvertently affecting sensitive resources. PIM also provides oversight for what users are doing with their administrator privileges.**

## What can you do with PIM?

**Today, you can use PIM with:**

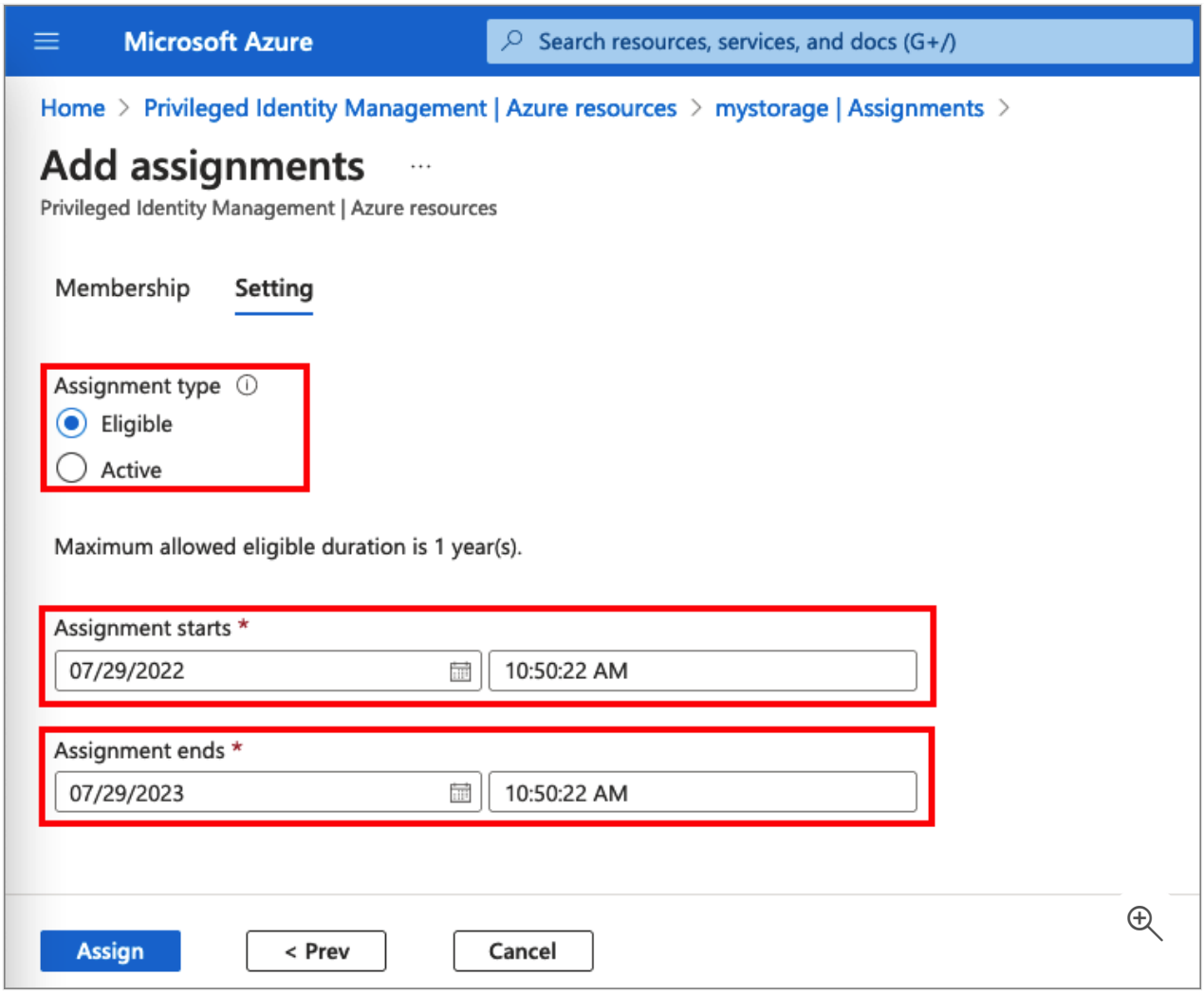
- **Microsoft Entra roles – Sometimes referred to as directory roles, Microsoft Entra roles include built-in and custom roles to manage Microsoft Entra and other Microsoft 365 online services.**
- **Azure roles – The role-based access control (RBAC) roles in Azure that grants access to management groups, subscriptions, resource groups, and resources.**

- **PIM for Groups – Provide just-in-time membership in the group and just-in-time ownership of the group. The Microsoft Entra Privileged Identity Management for Groups feature can be used to govern access to various scenarios that include Microsoft Entra roles, Azure roles, as well as Azure SQL, Azure Key Vault, Intune, other application roles, and third party applications.**

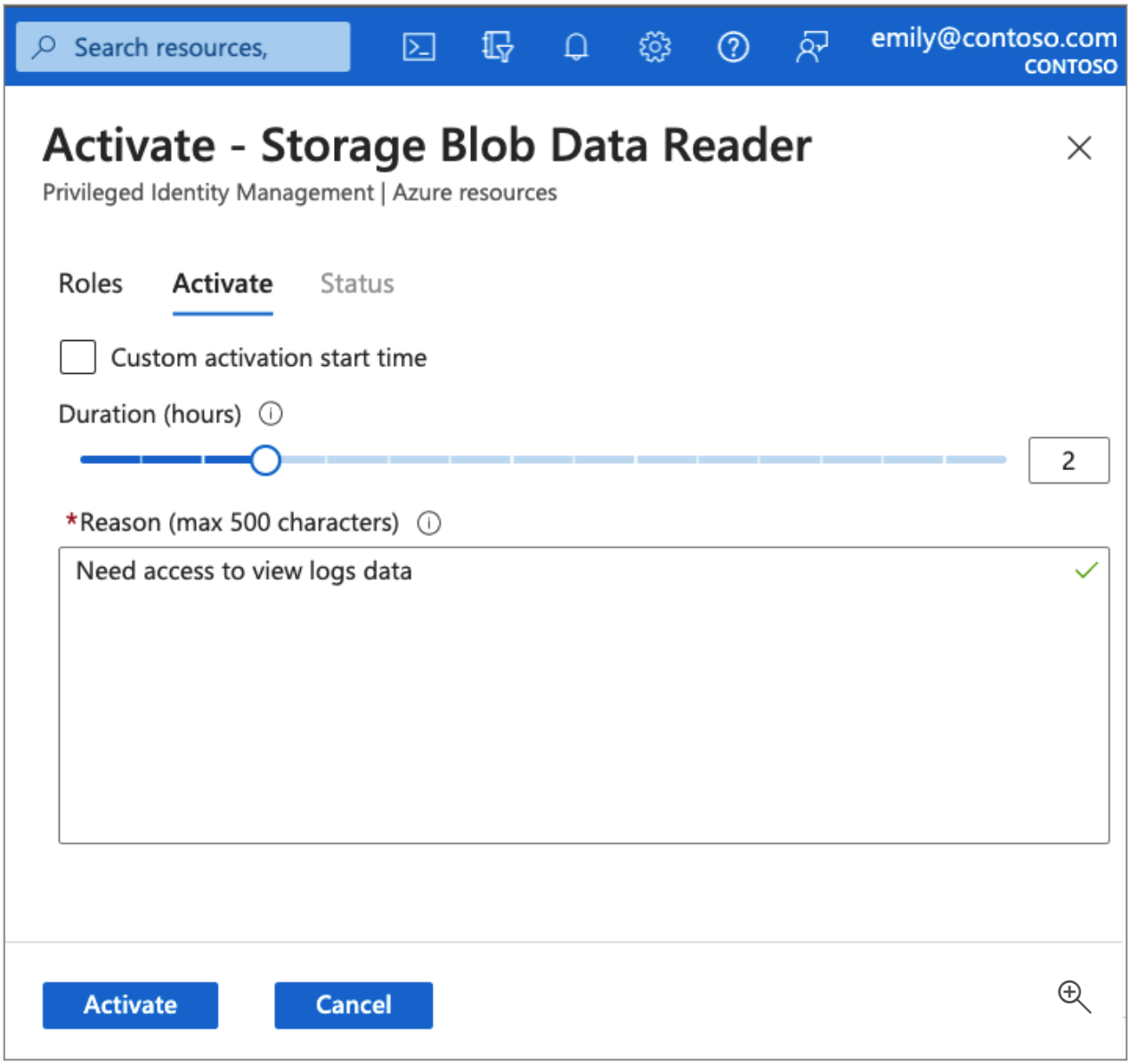
## General workflow

**There are a few steps that are generally part of a basic workflow when deploying PIM. These steps are: assign, activate, approve/deny, and extend/renew.**

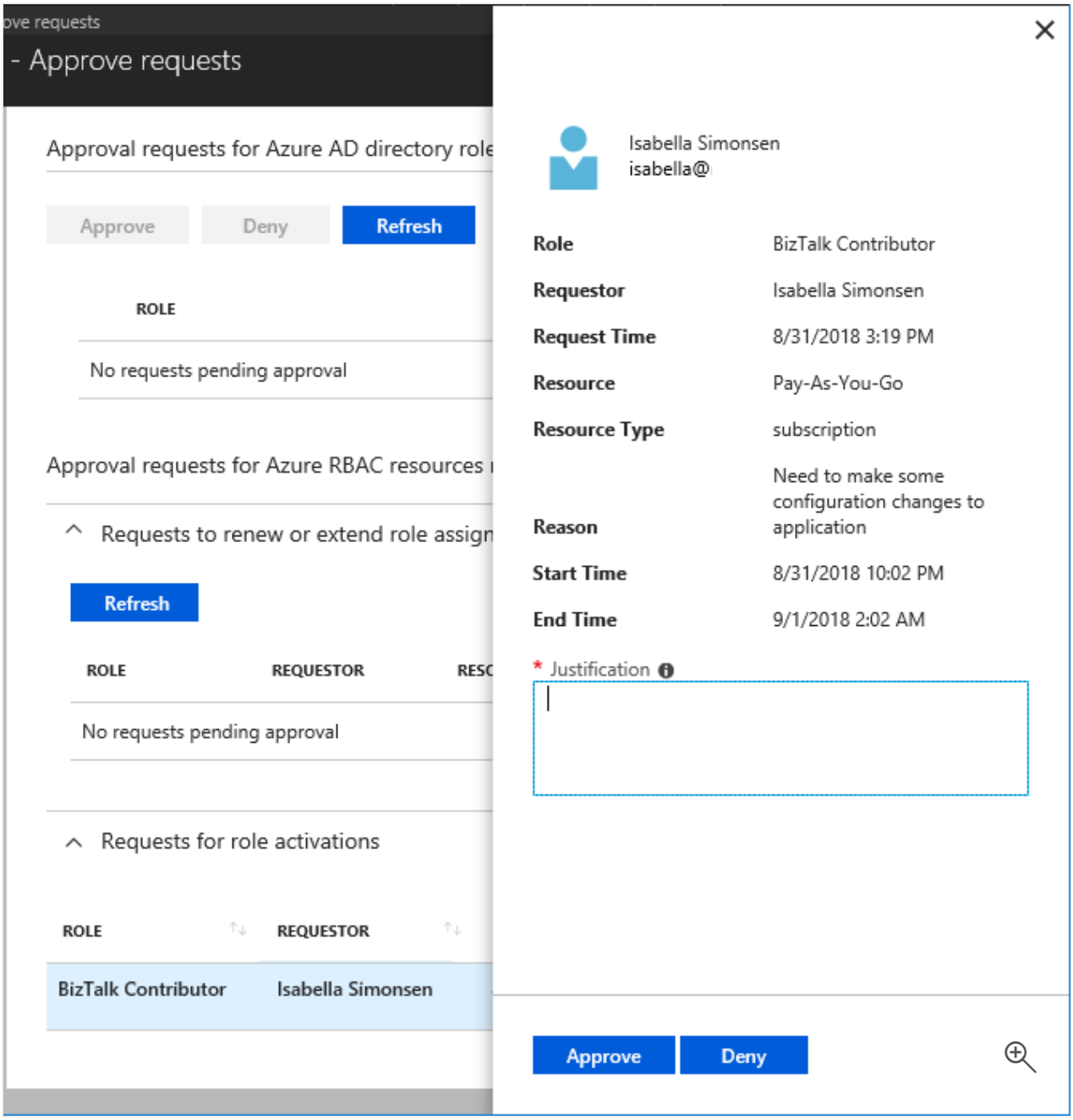
- **Assign - The assignment process starts by assigning roles to members. To grant access to a resource, the administrator assigns roles to users, groups, service principals, or managed identities. The assignment includes the following data:**
  - **Members or owners - The members or owners to assign to the role.**
  - **Scope - The scope limits the assigned role to a particular set of resources.**
  - **Assignment type - There are two options. Eligible assignments require the member of the role to perform an action to use the role. Actions might include activation, or requesting approval from designated approvers. Active assignments don't require the member to perform any action to use the role. Members assigned as active have the privileges assigned to the role.**
  - **Duration - The duration of the assignment is defined by start and end dates or is set to permanent.**



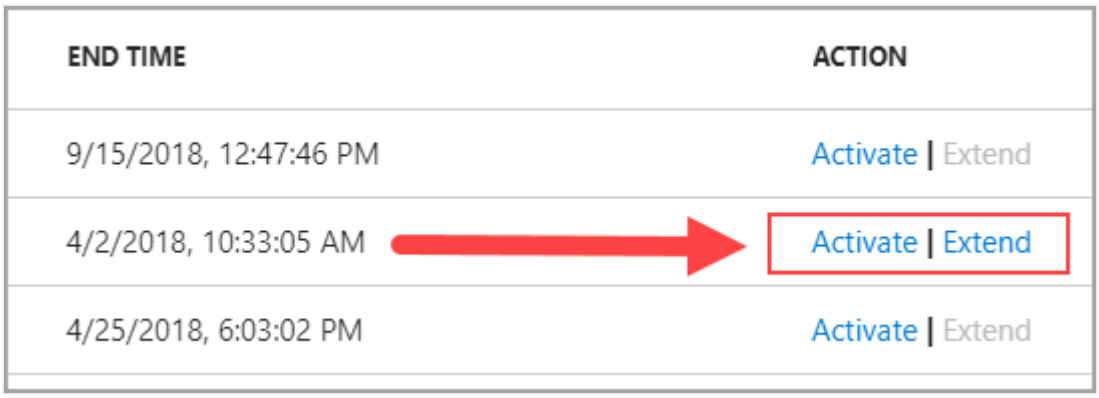

- **Activate - If users have been made eligible for a role, then they must activate the role assignment before using the role. To activate the role, users select specific activation duration within the maximum (configured by administrators), and the reason for the activation request.**




- **Approve or deny - Delegated approvers receive email notifications when a role request is pending their approval. Approvers can view, approve or deny these pending requests in PIM. After the request has been approved, the member can start using the role.**

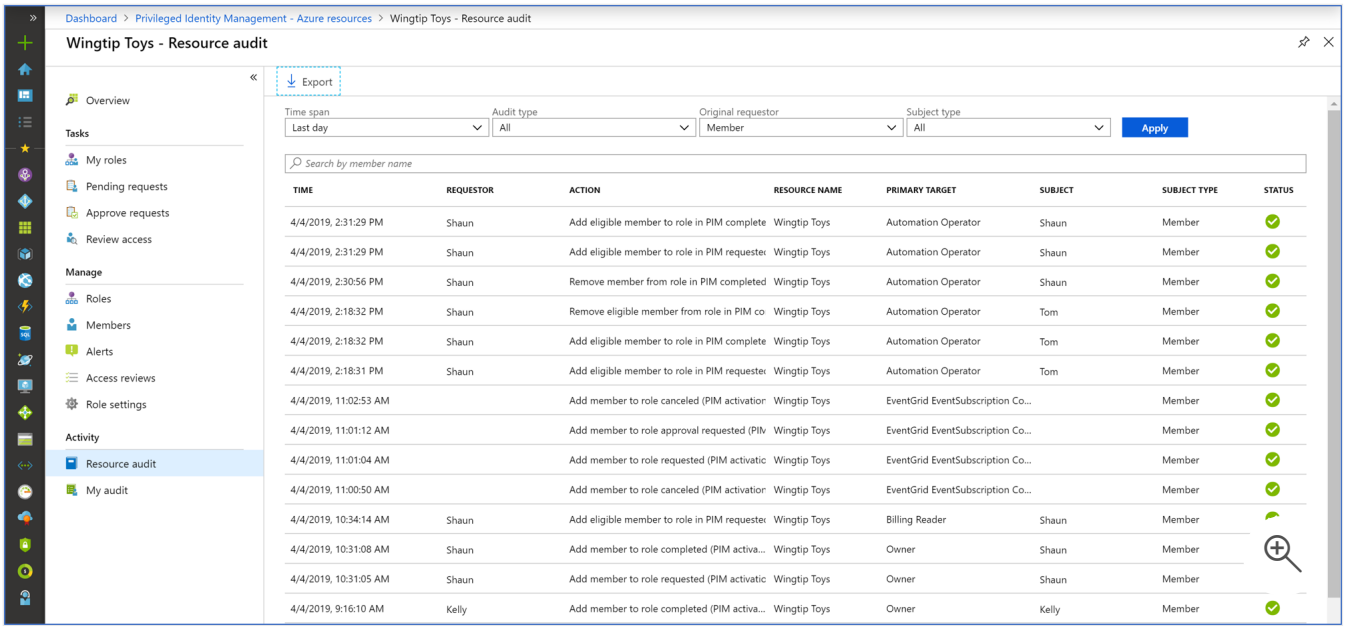



- **Extend and renew - When a role assignment nears expiration, the user can use PIM to request an extension for the role assignment. When a role assignment has already expired, the user can use Privileged Identity Management to request a renewal for the role assignment.**



# Audit

**You can use the Privileged Identity Management (PIM) audit history to see all role assignments and activations within the past 30 days for all privileged roles.**




# Next unit: Describe Microsoft Entra ID Protection

Continue >

**How are we doing?** ☆ ☆ ☆ ☆ ☆

100 XP

# Describe Microsoft Entra ID Protection

3 minutes

Identity Protection is a tool that allows organizations to accomplish three key tasks:

- Automate the detection and remediation of identity-based risks.
- Investigate risks using data in the portal.
- Export risk detection data to third-party utilities for further analysis.

Microsoft analyses trillions of signals per day to identify potential threats. These signals come from learnings Microsoft has acquired from their position in organizations with Microsoft Entra ID, the consumer space with Microsoft Accounts, and in gaming with Xbox.

The signals generated by these services are fed to Identity Protection. These signals can then be used by tools such as Conditional Access, which uses them to make access decisions. Signals are also fed to security information and event management (SIEM) tools, such as Microsoft Sentinel, for further investigation.

## Detect risks

With Identity Protection, risk can be detected at the user and sign-in level, can be categorized as low, medium, or high, and may be calculated in real-time or offline.

A sign-in risk represents the probability that a given authentication request isn't authorized by the identity owner. Here are just a few examples of the sign-in risks that Identity Protection in Microsoft Entra is able to identify:

- Anonymous IP address. This risk detection type indicates a sign-in from an anonymous IP address; for example, a Tor browser or anonymized VPNs.
- Atypical travel. This risk detection type identifies two sign-ins originating from geographically distant locations, where at least one of the locations may also be atypical for the user, given past behavior.
- Unfamiliar sign-in properties. This risk detection type considers past sign-in history to look for anomalous sign-ins. The system stores information about previous locations used by a user, and considers these "familiar" locations. The risk detection is triggered when the sign-in occurs from a location that's not already in the list of familiar locations.

- **Microsoft Entra threat intelligence. This risk detection type indicates sign-in activity that is unusual for the given user or is consistent with known attack patterns based on Microsoft's internal and external threat intelligence sources.**

**A user risk represents the probability that a given identity or account is compromised. Here are just a few examples of some of the user risks that Identity Protection in Microsoft Entra is able to identify:**

- **Anomalous user activity. This risk detection baselines normal administrative user behavior in Microsoft Entra, and spots anomalous patterns of behavior like suspicious changes to the directory.**
- **User reported suspicious activity. This risk detection is reported by a user who denied a multifactor authentication (MFA) prompt and reported it as suspicious activity. An MFA prompt that wasn't initiated by the user may mean that the user's credentials have been compromised.**
- **Leaked credentials. This risk detection type indicates that the user's valid credentials have been leaked. When cybercriminals compromise valid passwords of legitimate users, they often share those credentials. This sharing is typically done by posting publicly on the dark web, paste sites, or by trading and selling the credentials on illicit markets. When the Microsoft leaked credentials service acquires user credentials from the dark web, paste sites, or other sources, they're checked against Microsoft Entra users' current valid credentials to find valid matches.**
- **Microsoft Entra threat intelligence. This risk detection type indicates user activity that is unusual for the given user or is consistent with known attack patterns based on Microsoft's internal and external threat intelligence sources.**

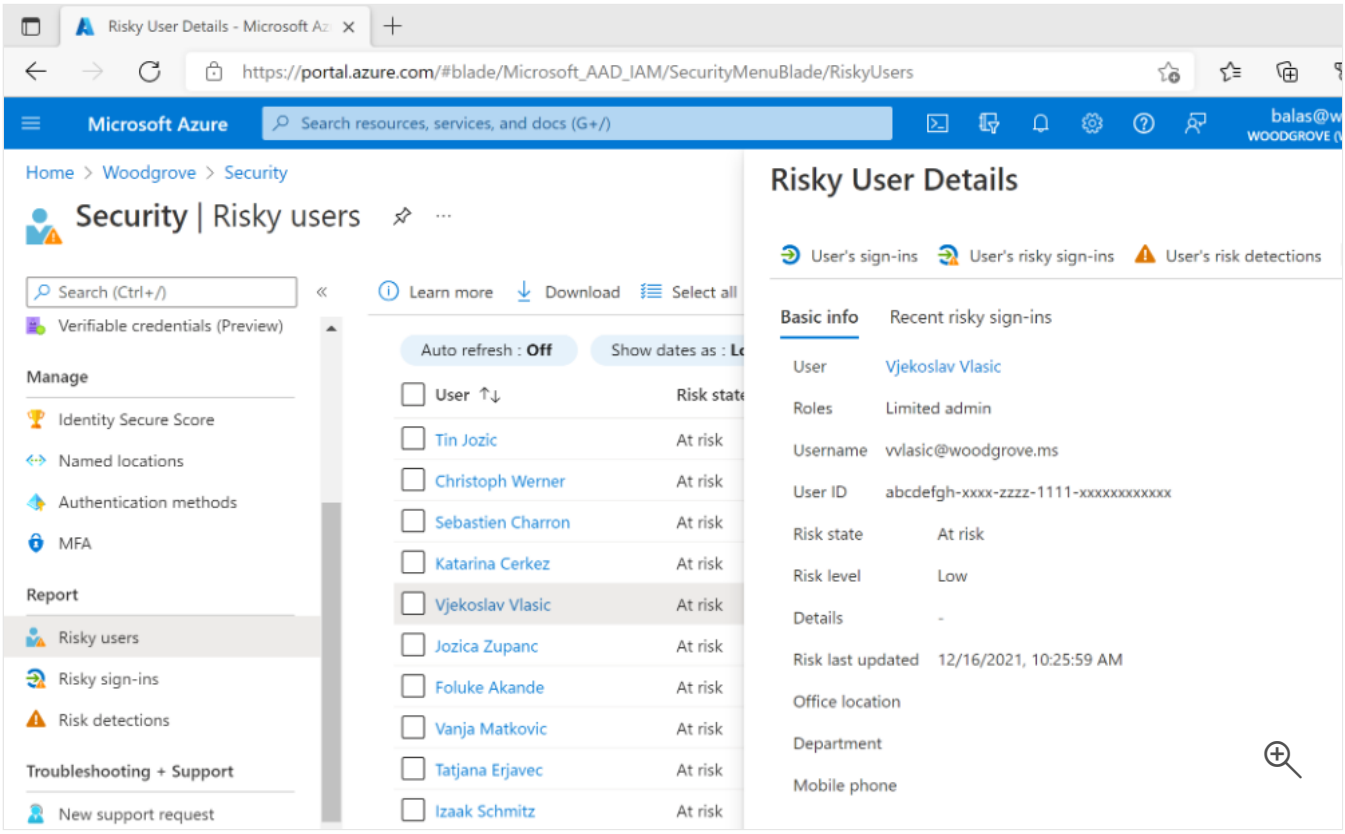
**Identity Protection only generates risk detections when correct credentials are used in the authentication request. If a user uses incorrect credentials, it will not be flagged by Identity Protection since there isn't a risk of credential compromise unless a bad actor uses the correct credentials. Risk detections can then trigger actions such as requiring users to provide multi-factor authentication, reset their password, or block access until an administrator takes action.**

## Investigate risks

**Identity Protection provides organizations with three reports that they can use to investigate identity risks in their environment. These reports are the risky users, risky sign-ins, and risk detections. Investigation of events is key to understanding and identifying any weak points in your security strategy.**

- **Risk detections: Each risk detected is reported as a risk detection.**

- **Risky sign-ins: A risky sign-in is reported when there are one or more risk detections reported for that sign-in.**
- **Risky users: A Risky user is reported when either or both of the following are true:**
  - **The user has one or more Risky sign-ins.**
  - **One or more risk detections have been reported.**




## Remediate

**After completing an investigation, admins will want to take action to remediate the risk or unblock users. Organizations can enable automated remediation using their risk policies. For example, risk-based conditional access policies can be enabled to require access controls such as providing a strong authentication method, perform multifactor authentication, or perform a secure password reset based on the detected risk level. If the user successfully completes the access control, the risk is automatically remediated.**

**When automated remediation isn't enabled, an administrator must manually review the identified risks in the reports through the portal, through the API, or in Microsoft 365 Defender. Administrators can perform manual actions to dismiss, confirm safe, or confirm compromise on the risks.**

## Export

**Data from Identity Protection can be exported to other tools for archive, further investigation, and correlation. The Microsoft Graph based APIs allow organizations to**

**collect this data for further processing in tools such as a SIEM. The data can also be sent to a Log Analytics workspace, archived data to a storage account, streamed to Event Hubs, or solutions.**

## Workload identity

**Microsoft Entra Identity Protection has historically protected users in detecting, investigating, and remediating identity-based risks. We're now extending these capabilities to workload identities to protect applications and service principals.**

**A workload identity is an identity that allows an application or service principal access to resources. These workload identities differ from traditional user accounts as they:**

- **Can’t perform multifactor authentication.**
- **Often have no formal lifecycle process.**
- **Need to store their credentials or secrets somewhere.**

**These differences make workload identities harder to manage and put them at higher risk for compromise.**

**Microsoft Entra ID Protection helps organizations manage this risk by providing workload identity risk detections across sign-in behavior and other indicators of compromise.**

---

## Next unit: Describe Microsoft Entra Permissions Management

Continue >

---

**How are we doing?** ☆ ☆ ☆ ☆ ☆

100 XP

# Describe Microsoft Entra Permissions Management

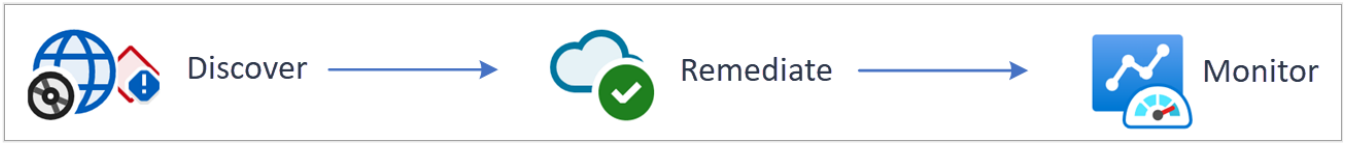
3 minutes

**Microsoft Entra Permissions Management is a cloud infrastructure entitlement management (CIEM) product that provides comprehensive visibility and control over permissions for any identity and any resource in Microsoft Azure, Amazon Web Services (AWS) and Google Cloud Platform (GCP).**

**This functionality helps organizations address the Zero Trust principle of least privilege access. Organizations need to consider permissions management as a central piece of their Zero Trust security strategy that includes implementing least privilege access across their entire infrastructure. Some of the key reasons include:**

- **Organizations are increasingly adopting multicloud strategy and are struggling with the lack of visibility and the increasing complexity of managing access permissions.**
- **With the proliferation of identities and cloud services, the number of high-risk cloud permissions is exploding, expanding the attack surface for organizations.**
- **IT security teams are under increased pressure to ensure access to their expanding cloud estate is secure and compliant.**
- **The inconsistency of cloud providers' native access management models makes it even more complex for Security and Identity to manage permissions and enforce least privilege access policies across their entire environment.**

**Permissions Management detects, automatically right-sizes (remediates), and continuously monitors unused and excessive permissions.**
**Permissions Management helps organizations address requirements for least access privilege through discovery of the entire infrastructure, remediation that automatically rightsizes for least privilege access, and continuously monitoring the entire infrastructure for unused and excessive permissions.**




## Discover

**Customers can assess permission risks by evaluating the gap between permissions granted and permissions used.**

- **Cross-cloud permissions discovery: Granular and normalized metrics for key cloud platforms: AWS, Azure, and GCP.**
- **Permission Creep Index (PCI): An aggregated metric that periodically evaluates the level of risk associated with the number of unused or excessive permissions across your identities and resources. It measures how much damage identities can cause based on the permissions they have. Permission usage analytics: Multi-dimensional view of permissions risk for all identities, actions, and resources.**

## Remediate

**Customers can right-size permissions based on usage, grant new permissions on-demand, and automate just-in-time access for cloud resources.**

- **Automated deletion of permissions unused for the past 90 days.**
- **Permissions on-demand: Grant identities permissions on-demand for a time-limited period or an as-needed basis.**

## Monitor

**Customers can detect anomalous activities with machine learning-powered (ML-powered) alerts and generate detailed forensic reports.**

**ML-powered anomaly detections. Context-rich forensic reports around identities, actions, and resources to support rapid investigation and remediation. Permissions Management deepens Zero Trust security strategies by augmenting the least privilege access principle, allowing customers to:**

- **Get comprehensive visibility: Discover which identity is doing what, where, and when.**
- **Automate least privilege access: Use access analytics to ensure identities have the right permissions, at the right time.**
- **Unify access policies across infrastructure as a service (IaaS) platforms: Implement consistent security policies across your cloud infrastructure.**

**Once your organization has explored and implemented the discover, remediation and monitor phases, you've established one of the core pillars of a modern zero-trust security strategy.**

---

# Next unit: Describe Microsoft Entra Verified ID

Continue >

**How are we doing?** ☆ ☆ ☆ ☆ ☆

100 XP

# Describe Microsoft Entra Verified ID

3 minutes

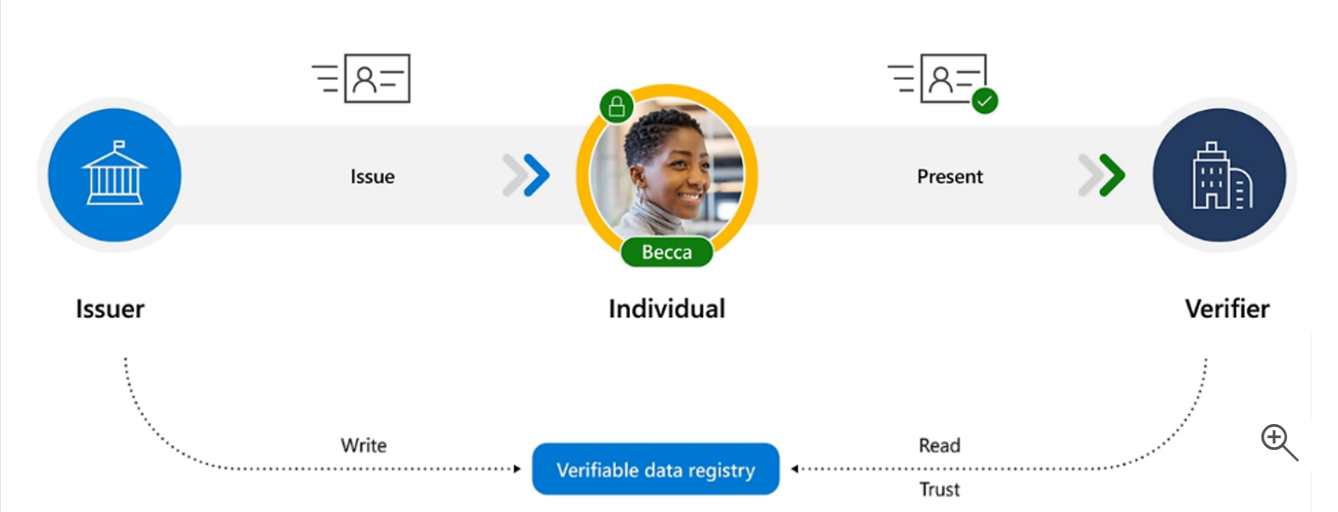
**Microsoft Entra Verified ID is a managed verifiable credentials service based on open standards. Verified ID automates verification of identity credentials and enables privacy-protected interactions between organizations and users.**

## Why do we need it?

**In the digital world, transactions are increasingly done over the web and often require individuals to make claims or assertions that organizations can digitally verify. The current process of obtaining and presenting a digital credential that can make the minimum required claims and that can be verified can be difficult and cumbersome. A digital credential serves as a digital identity. Once you use that online digital identity to access the desired service or make an online transaction, it's common you begin to get targeted advertisements and emails for services for which you never signed up. That's because it's hard to retain control of your identity once you've shared it in exchange for access to a service. Individuals and businesses need a way to express their qualifications and/or personal information, that is, our digital identities, over the web in a manner that is cryptographically secure, compliant to privacy requirements, and machine readable for verification. Additionally, individuals and organizations want to be able to control how and when their digital identities are used and shared. Verifiable credentials help address these challenges.**

## How it works

**This diagram illustrates the participation of three parties in a verifiable credential's interaction. This solution automates verification of identity credentials and claims.**




- **The issuer is an organization that attests to claims and grants digitally signed credentials to the user. An issuer can be an identity verification provider, a government agency, an employer, a university, or any other organization that can provide proof of the user's credential.**
- **The user receives and approves the credentials obtained from the issuer, stores and manages credentials in their digital wallet, and presents it to the verifier. The credential claims are cryptographically signed with the user's private key.**
- **The verifier is an organization that requests proof and, upon receipt, verifies that the claims in the credentials satisfy requirements. A verifier could be a prospective employer, and airline, mortgage company, or any organization that is requesting proof of the user's credential.**

**Supporting it all is a verifiable data registry. The underlying verifiable data registry is a collection of systems involved in creating and recording meta data that are used with verifiable credentials, including public keys. These systems are usually distributed networks, such as distributed ledgers, blockchains, distributed file systems, or other trusted data storage. The way to think about the verifiable data registry is as an underlying network that represents a trust system. The verifier interacts with the data registry to read the meta-data associated with the credential to then verify the credential that presented by the user.**

**A common scenario with any credential is that the credential may expire, or the issuer may need to revoke that credential. The standard for verifiable credentials includes property fields in the credential to account for these scenarios.**

**Visit https://aka.ms/vcdemo for a more complete demonstration of an onboarding verifiable credential scenario. Also, the summary and resources section of this module includes a link to the training content that describes concepts behind Microsoft Entra Verified ID.**

---

# Next unit: Knowledge check

Continue >

**How are we doing?** ☆ ☆ ☆ ☆ ☆

100 XP

# Summary & resources

1 minute

**In this module, you learned how Microsoft Entra provides tools to help you protect and govern identities. You learned about identity life-cycle management and how Identity Protection can detect potential identity risks. Finally, you learned how solutions such as access reviews, privileged identity management, and permissions management all help organizations adhere to the concepts of least privilege access, a core principle of a Zero Trust security strategy.**

**Now that you've completed this module, you'll be able to:**

- **Describe the identity governance capabilities of Microsoft Entra.**
- **Describe Privileged Identity Management (PIM).**
- **Describe the capabilities of Microsoft Entra ID Protection.**
- **Describe permissions management.**

## Learn more

**For more information about the topics raised in this module, see:**

- **What is Microsoft Entra ID Governance?**
- **Microsoft Entra access reviews**
- **What is entitlement management?**
- **Azure terms of use statements**
- **Microsoft Entra Privileged Identity Management**
- **What is Identity Protection?**
- **What's Permissions Management?**
- **Describe the concepts behind Microsoft Entra Verified ID**

## Module incomplete:

Go back to finish

**How are we doing?** ☆ ☆ ☆ ☆ ☆